1-1-2003

Assessment of HIPAA compliance: a comparison study of current implementations

Kurtis Alan Ness
Iowa State University

Assessment of HIPAA compliance: A comparison study of current implementations

by

Kurtis Alan Ness

A thesis submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Sree Nilakanta, Major Professor
Jennifer Davidson
Troy Strader

Iowa State University
Ames, Iowa
2003

Graduate College
Iowa State University

This is to certify that the master's thesis of

Kurtis Alan Ness

has met the thesis requirements of Iowa State University

Signatures have been redacted for privacy

TABLE OF CONTENTS

ABSTRACT

The Health Insurance Portability and Accountability Act (HIPAA) is a set of federally mandated regulations passed down to the healthcare industry in an attempt to simplify administrative procedures and reform the insurance market. HIPAA intends to provide healthcare savings by reducing administrative costs by standardizing electronic administrative processes throughout the healthcare industry. It also intends to protect individual privacy from outside agencies with tough new privacy and security measures that include physical security as well as electronic security.

As healthcare organizations attempt to become complainant with the new regulations a deadline for HIPAA compliance looms nearer threatening the organizations with the possibility of fines for infractions of the federal regulations. The National Committee on Vital Health and Statistics (NCVHS) recently commented that they were surprised and disturbed by high levels of confusion and frustration regarding the compliance efforts of healthcare providers.

In this thesis research is performed to assess the HIPAA readiness of local healthcare providers, specifically Mercy, Methodist, Broadlawns and Mary Greeley hospitals. The data collected from these healthcare organizations is used to compare and contrast the local organizations with each other and against a national benchmark. The results of this comparison show differences within each local health care organizations approach to HIPAA compliance, their concerns and overall perceptions of the HIPAA Act of 1996. Another result of this thesis is an assessment of local HIPAA readiness is relation to national levels of compliance.

CHAPTER 1 INTRODUCTION

1.1 Overview

The Health Insurance Portability and Accountability Act (HIPAA) is a set of federal regulations signed into law August 21,st 1996 designed to reform the healthcare industry. The implementation of HIPAA is performed in phases including deadlines for when compliance must be reached.

As the April 14th 2003 deadline for HIPAA compliance approaches, healthcare organizations are at many different levels of readiness. The National Committee on Vital and Health Statistics (NCVHS), a committee that monitors the implementation of the Administrative Simplification provisions of HIPAA, reported on September 27, 2002 in a letter to Tommy Thompson, the Secretary of Health and Human Services, that "...the NCVHS was both surprised and disturbed at the generally low level of implementation activities and the high levels of confusion and frustration"[1].

The cost of implementing HIPAA regulations may be significant for a healthcare organization and fines for violating the regulations can go as high as $250,000. For general failure to comply, however, the fine is a more modest $100 per incident with the maximum for "general failure to comply" set at $25,000. The larger fines are reserved for grosser violations such as wrongful disclosure - $50,000, offense under false pretenses - $100,000 and offense with intent to sell information with carries the largest $250,000 fine.

The HIPAA act is predicted to save money, however, by reducing administrative costs. Currently it is estimated that for every dollar spent in health care 26 cents goes to cover administrative costs. The HIPAA act is expected to cut these costs down to five cents [2].

1.2 - Research Objective

The HIPAA act is a large complex piece of legislature and the implementation of its federal mandates have many health care professionals and government officials concerned about the impending compliance date. As mentioned by the NCVHS, problems have been noted regarding implementation of HIIPAA regulations. The object of this paper is to analyze and get an understanding of Iowa hospitals, HIPAA compliance readiness, compare them with each other and to the national average to observe similarities and discrepancies. The hospitals that will be assessed are Methodist Hospital in Des Moines, Mercy Hospital in Des Moines, Mary Greeley Hospital in Ames, and Broadlawns Hospital in Des Moines. The assessment data for these local hospitals will be analyzed, compared, and contrasted with each other and also against data gathered from the Phoenix Health Care Systems National Survey for Fall 2002.

1.3 – Thesis Organization

Chapter 1 introduces the research problem. Following the introduction a brief history of HIPAA regulations is given to provide the motivation for the research. Here, the major sections and topics of HIPAA are presented. After the background section the results of a survey taken of local hospitals are introduced including discussion about the similarities and differences among the gathered data. After analysis of the local survey, a comparison of the local survey results with data obtained from a nation national survey is presented. Subsequently, a conclusion is given that highlights the findings of the research and comments on possibilities for future research.

CHAPTER 2 – BACKGROUND OF HIPAA

2.1 A Brief History

HIPAA is a broad set of regulations aimed reforming and streamlining current practices in the health care industry. In the early 1990's the administration under then President Bush took an in-depth look at the health care industry in an attempt to locate ways to reduce costs. A group of health care industry leaders such as the President of the Blue Cross and Blue Shield Association and the Health Insurance Association of America was formed to try and meet this challenge, arriving at the conclusion that the best way to reduce costs was to increase the use of EDI (electronic data interchange) to perform transactions. This group later became known as the Workgroup for Electronic Data Interchange or WEDI.

WEDI later suggested that in order for the EDI system to work correctly a set of standards should be met for the data to be transmitted effectively and securely. A federal attempt to reach such standards is the beginning of the HIPAA act and has become a much more involved and ambitious piece of legislation.

2.2 - Major Titles and Sections of HIPAA

HIPAA legislation is broken into five major titles, which include:

1. Title 1 – Health Insurance Reform
2. Title 2 – Administration Simplification
3. Title 3 – Tax related Health Provisions
4. Title 4 – Application and Enforcement of Group Health Plan Requirements
5. Title 5 – Revenue Offsets

The nine major sections of HIPAA are:

1. Group Market Portability (Title I, Subtitle A)

2. Individual Market Portability (Title I, Subtitle B)
3. Medical Savings Accounts (Title III, Subtitle A)
4. Long Term Care Tax Clarification and Consumer Protection (Title III, Subtitle C)
5. Tax Deductibility for the Self-employed (Title III, Subtitle B)
6. Fraud and Abuse Prevention (Title II, Subtitles A - E)
7. Administrative Simplification (Title II, Subtitle F)
8. Medicare Duplication and Coordination (Title II, Subtitle G)
9. Accelerated Death Benefits (Title III, Subtitle D).

This paper will focus on the Administration Simplification Title due to the complexity of its regulations.

Title 2 or the Administration Simplification section of HIPAA requires the "Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care"[3].

This definition can be further broken down into four sections:

1. Electronic Health Transactions Standards
2. Unique Identifiers
3. Security and Electronic Signature Standards
4. Privacy and Confidentiality Standards

2.2.1 Electronic Health Transaction Standards

Currently health care providers use many different electronic formats to send and receive patient data. Because of the different formats it is difficult to use EDI as a primary

form of transaction activity as many business partners use incompatible systems. A significant savings, an estimated 21 cents for every dollar spent on health care, can be realized once the compatibility issue has been addressed, allowing health care organizations to communicate with other health care organizations and various business partners using EDI as a primary source of transactions. The American National Standards Institute (ANSI) will be addressing and developing the common EDI format to be adopted by the health care industry.

A set of codes must also be developed, as required by HIPAA, to reduce mistakes and duplication of administrative tasks and costs. This set of codes are already widely accepted and used by most members of the health care industry.

2.2.2 - Unique Identifiers

Currently identifiers are used within the health care industry that are not unique which may lead to confusion and administrative mistakes. By using unique identifiers HIPAA legislators hope that mistakes may be minimized.

2.2.3 - Security and Electronic Signature

With the increase in sensitive information being sent electronically, new security measures need to be addressed in order to ensure the confidentiality, integrity and availability of health care data, especially individually identifiable data. HIPAA regulations are vague about this area as technology is moving too quickly to mandate specific types of technology to use. However, some standards are in place to protect physically stored information, electronically stored information, as well as access to and daily maintenance of individual identifying information.

2.2.4 - Privacy and Confidentiality

Perhaps the most controversial of the Administrative Simplification sections is the privacy rules. The privacy rules were designed to:

1. Limit the non-consensual use and release of private health information
2. Give patients new right to access their medical records and to know who else has accessed them
3. Restrict most disclosure of health information to the minimum needed for the intended purpose
4. Establish new criminal and civil sanctions for improper use or disclosure
5. Establish new requirements for access to records by researchers and others. [4].

There are five basic principles that are reflected in the above regulations that must be observed and they are:

1. Consumer Control: The regulation provides consumers with critical new rights to control the release of their medical information
2. Boundaries: With few exceptions, an individual's health care information should be used for health purposed only, including treatment and payment
3. Accountability: Under HIPAA, for the first time, there will be specific federal penalties if a patient's right to privacy is violated
4. Public Responsibility: The new standards reflect the need to balance privacy protections with the public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care and fighting health care fraud and abuse
5. Security: It is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure [5].

Currently the American Association of Physicians and Surgeons (AAPS) have sued the federal government in an attempt to halt the implementation of the privacy rules.

They maintain that because the new rules allow the government to access medical records without patient consent or a warrant, that these rules do not promote privacy and that they create "privacy loopholes" that make individually identifiable patient records even less private than before the HIPAA rules. The AAPS and many other healthcare organizations and politicians have a long list of grievances against this set of regulations (http://aapsonline.org).

Since the changes in the final privacy rules, there has been a lot less controversy, however the AAPS will continue their lawsuit, which is currently on appeal after being dismissed by a federal judge. Other plaintiffs against the DHHS in the AAPS lawsuit include Representative Ron E. Paul, a republican from Texas.

Another politician against the HIPAA privacy regulations is House Majority Leader Dick Armey who stated, "It started out as a modest little bill, claiming to make coverage portable from job to job. It grew.... It ... did little to make insurance more affordable, but it did set a dangerous precedent for federal regulation of health insurance. *And, it appears to have expanded bureaucrats' access to our medical records without a search warrant.* Mr. Armey added that, "Not only was I awake when HIPAA came up, but I voted for it.... I cast a bad vote. I feel bad about it"[6].

In spite of the actions being taken to halt the nationwide implementation of HIPAA regulations it appears that they are here to stay. In the next section, we will take a look at local hospitals and their approach to implement HIPAA regulations.

CHAPTER 3 – LOCAL SURVEY RESULTS

Four local hospitals were involved with the survey: Methodist, Mercy, Broadlawns and Mary Greeley. Methodist and Mercy hospitals both have more than 400 beds in their organization whereas Broadlawns and Mary Greeley have between 100 and 400 beds. The information was gathered from security officers and HIPAA coordinators from the IT department of each hospital.

1. Methodist (400+)
2. Mercy (400+)
3. Broadlawns (100 – 400)
4. Mary Greeley (100 – 400)

Empirical data was gathered in an attempt to discover the level of HIPAA compliance as of Fall 2002. Over a hundred questions were asked to get a clear understanding of each organization's current situation about the HIPAA regulations.

Table 1. Break out of locally surveyed hospitals

Hospital of 100 - 400 beds	2	50%
Hospital of 400+ beds	2	50%

Table 2. Has your organization completed HIPAA transactions and code sets remediation and privacy remediation?

Hospital Size	100 - 400	400+
YES	0%	0%
NO	100%	100%

Table 3. None of the polled respondents have completed Transactions/Code Sets and Privacy remediation but were asked anyway what part of the process is the most troublesome?

100 - 400	400+	
25%	0%	Enterprise-Wide HIPAA Project Coordination
0%	0%	Finding Sufficient, qualified staff
0%	25%	Resolving issues with 3rd parties (vendors, bus. Assocs.)
0%	0%	Achieving adequate funding
25%	25%	Understanding/ interpreting legal requirements
0%	0%	Achieving successful integration of new policies & procedures
0%	0%	Other

Table 4. What HIPAA compliance activities is your organization currently engaged in? (Check all that apply).

100 - 400 beds	T&CS	Unique Ids	Security	Privacy
Awareness/General HIPAA Education	25%	50%	50%	25%
Assessment	0%	0%	25%	0%
Project Planning	25%	0%	0%	25%
Implementation	25%	0%	25%	25%
Training	25%	0%	0%	25%

Table 4. (continued)

400+	T&CS	Unique Ids	Security	Privacy
Awareness/General HIPAA Education	0%	0%	25%	25%
Assessment	0%	25%	25%	25%
Project Planning	25%	0%	50%	25%
Implementation	25%	25%	0%	50%
Training	0%	0%	0%	0%

3.1 – Similarities

3.1.1 – Standard Identifier Questions

All surveyed hospitals reported that they were in the Planning stages concerning the review and remediation of all duplication errors contained within their Master Patient Index. Three of the four reported that they have not started the integration of their assigned National Provider Identifier for each area within their organization and verified each with all payers their organization works with, as well as all medical providers. Mercy Hospital is the organization that reported that they were currently in the planning stages.

3.1.2 – Electronic Transactions and Code Sets

All four polled hospitals reported similarly when asked if they had taken steps to ensure that all HIPAA covered electronic transactions conducted by their organization are sent using the proper ANS ASC X12N standards as required, stating they were currently "in progress".

3.1.3 – Security

Similar results reported regarding HIPAA compliant policies with all four respondents stating that they are currently "in progress" regarding the development of said securities as they apply to the organizations data and physical security. "In progress" was also reported by all four hospitals concerning policies and procedures that require control over the monitoring of and documentation of unauthorized access to individually identifiable health information.

All four hospitals were asked how far they considered their organization to have progressed towards completion of its HIPAA compliance implementation project with all four answering that they were in the "in progress" category.

3.1.4 – Privacy

The most striking similarities were found in the privacy section of HIPAA compliance with all four hospitals responding identically for every question. Seven questions were asked with all four respondents reporting to be in the "in progress" phase of remediation.

Another survey asked the respondents when they believed they would be finished with the privacy remediation with 3 of the four hospitals reporting that they would be finished in the next 4 to 6 months, in time for the federally mandated deadline for privacy remediation. Mary Greeley reported that they had filed for an extension and that they would expect to complete privacy remediation within the next 10 to 13 months, which would meet the extended deadline for privacy remediation.

3.1.5 – Roadblocks to HIPAA Compliance

When asked to put in order (with 1 being the most challenging a 6 the least) the roadblocks to compliance all four hospitals responded with "interpretation of regulations" as the single most challenging roadblock.

Three of the four hospitals reported that they believe that "inadequate expertise available" as the least challenging roadblock to HIPAA compliance with Mary Greeley having the on exception reporting that they believed it to be the third most challenging. Mary Greeley considered vendor compliance to be the least challenging roadblock to compliance.

3.2 – Differences

3.2.1 – Electronic Transactions and Code Sets

The largest discrepancy regarding Electronic Transactions and Codes sets occurred when the survey question was asked, "Have appropriate mechanisms been developed and implemented to effectively monitor your organization's compliance with official coding guidelines?". Mercy reported that they were only in the "planning" stages with Methodist stating that they were in the "in progress" stage. The two smaller hospitals, Mary Greeley and Broadlawns, reported that they had "finished" with this aspect of Electronic Transactions and Code Sets remediation.

Another discrepancy between the larger and small hospitals was observed when the question was asked, "Have you developed a plan for, implemented, and documented regular training sessions for your coding staff on current coding practices as required by HIPAA?". The larger hospitals, Mercy and Methodist, reported that they had "not started" with Mary Greeley and Broadlawns both jumped past the "planning" phase and were in the "in progress" phase of compliance.

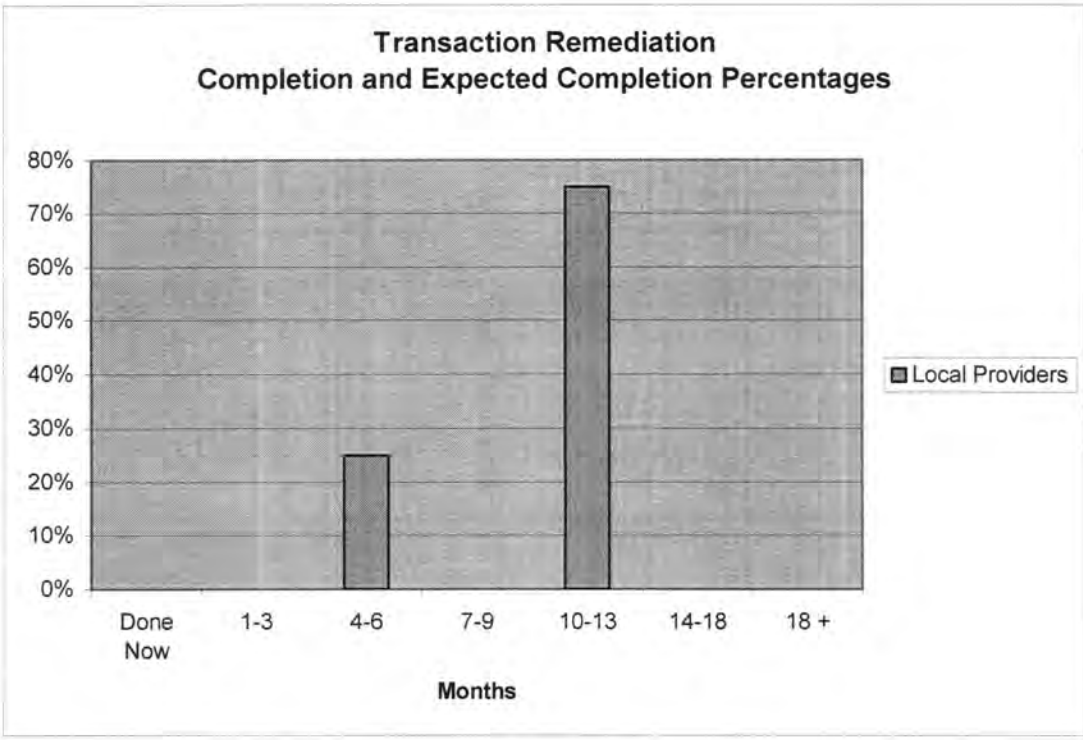


Figure 1. Three of the four polled local hospitals reported that they expected to have Transaction/Code Set remediation completed between 10 and 13 months from November 2002. Only one of the local hospitals believed that they would be done in the next four to six months.

3.2.2 – Security

Three questions resulted in discrepancies regarding security remediation. Regarding policies and procedures to review potential employees using appropriate screening and background checks, Methodist reported that they were in the "planning" phase, Mary Greeley in the "in progress" phase and Mercy and Broadlawns in the "finished" phase of compliance.

Overall security of the surveyed organizations automated systems rooms are in varying levels of testing and documentation. Mary Greeley reporting to be in the "planning" phase, Methodist in the "in progress" phase and Mercy and Broadlawns in the "finished" phase of compliance.

Finally regarding the development and approval of compliant policies and procedures addressing appropriate back-up and complete disaster recovery we found different levels of compliance with Mary Greeley in the "planning" phase, Methodist and Mercy are both in the "in progress" phase with only Broadlawns reporting to be in the "finished" section of remediation.

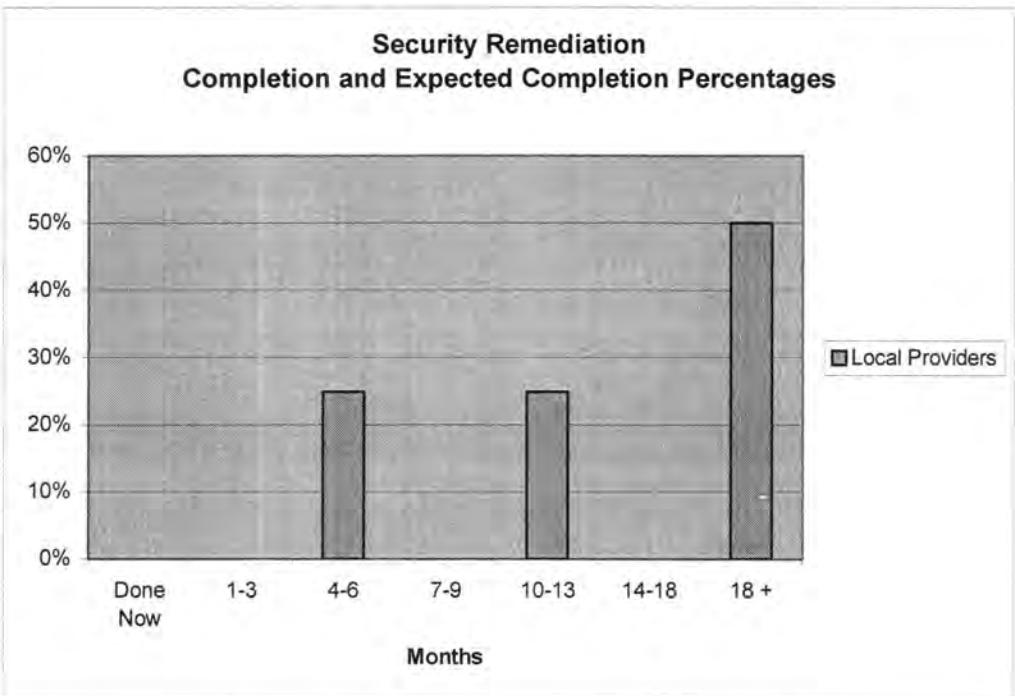


Figure 2. Two of the local healthcare providers expect that it will take them longer than 18 months before they will be able to comply with HIPAA Security regulations. One of the local hospitals believes that they will be compliant with in the next ten to thirteen months with another hospital expecting compliance in the next four to six months.

3.2.3 – Privacy

The only discrepancy regarding privacy remediation was that Mary Greeley hospital applied for and extension and is expecting to take 10 to 13 months to comply. The other three hospitals are expecting to complete privacy remediation with in the next 4 to 6 months, in time for the privacy remediation deadline.

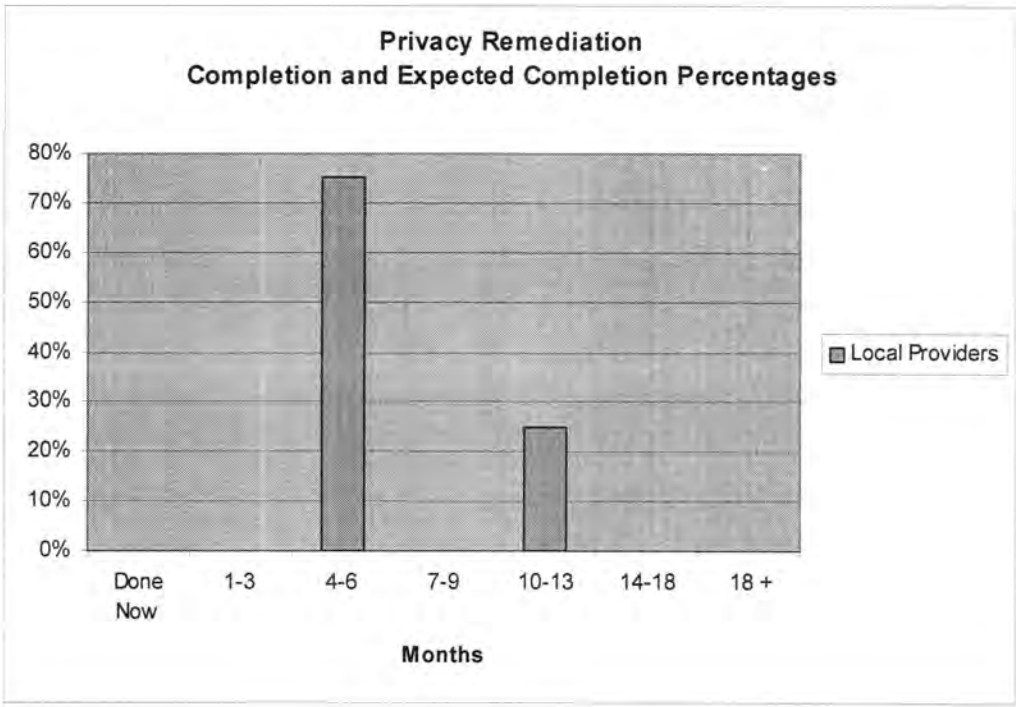


Figure 3. Three or the four polled local hospitals believe that they will be finished with HIPAA Privacy remediation in the next four to six months with one local hospital reporting an estimated ten to thirteen months before compliance.

3.2.4 – Budget

During 2002 the hospitals estimated very different numbers regarding the amount of money that has been and will be spent on reaching HIPAA compliance. Broadlawns hospital responded that they expect to spend $50,000 to $100,000 while attempting to reach compliance; Mercy reported that they expect to spend $100,00 to $250,000 on compliance activities with Mary Greeley reporting the largest amount of $500,000 to $1,000,000 in spending. Methodist hospital reported that they did not know what they expect to spend during 2002.

During 2002, Mercy, Mary Greeley and Broadlawns hospitals expected to spend between $600,000 and $1,200,000 in reaching compliance. For 2003 they estimated total is in the range of $150,000 and $300,000.

The maximum amount of money spent by all local hospitals in reaching compliance is predicted to be (2002 – 2003) is $1,650,000. The least amount of money needed to reach compliance is predicted to be $800,000 by Mercy, Mary Greeley and Broadlawns hospitals.

3.2.5 – Support from Senior Management and Department Heads

Support for enterprise HIPAA compliance initiatives among senior management and department heads varied among the respondents. With a range of responses for support from one (low) to five (high), only one hospital (Methodist) reported to receive level five support from their senior management and department heads. The next highest was level four support from Broadlawns senior management and department heads and level three support was reported for both Mercy and Mary Greeley.

During an interview with Mary Greeley a question was asked regarding what (if anything) they would do change to make HIPAA easier to implement. The answer was to get rid of it all together. Shawn Steffen, the IT manager at Mary Greeley, stated that he believed that HIPAA has become something it was not intended to become. Mr. Steffen stated he, "doesn't believe that politicians know what they are doing." adding that they are, "creating confusion and increasing paper work". He also believes that HIPAA regulations will have and are having a negative affect on healthcare quality by creating confusion with the unclear privacy regulations. Mr. Steffen stated that HIPAA has grown "outside its realm" and will no longer be able to achieve the benefits that healthcare organization were expected to realize as a result of HIPAA compliance. Mercy Hospital reported that they do not have strategic goals focused on realizing benefits from its HIPAA compliance efforts. Mercy Hospital also reported a low support level (level 3) from senior management and department heads along with Mary Greeley.

3.2.6 - Roadblocks to HIPAA Compliance

Concerning roadblocks to HIPAA compliance Mercy hospital did not report budget constraints as very troublesome rating it a level 5 with 6 being the least troublesome. Mercy hospital, however, is owned by a parent company that provides strong support for HIPAA compliance. Dennis Potter, IT director for Mercy Hospital, stated that the leadership from Mercy's parent company as one of their strong areas in reaching HIPAA compliance with most of the policies being written and provided by the parent company.

Mary Greeley, however, rated budget constraints at level 2 the second most troublesome aspect of HIPAA compliance. Methodist who perceived senior management support at the highest level (level 5) reported budget constraints as second lowest (level 5). Broadlawns who reported level 4 support from senior management, reported budget constraints as the fourth most troublesome aspect to HIPAA compliance.

3.3 – Effects on Business Processes

3.3.1 – Internal Business Processes

The effects of HIPAA are being felt in several internal processes. During an interview with Shawn Steffen, Director of the Business Office, Medical Records at Mary Greeley Hospital stated that he was concerned about the physical control of patient charts. It has been common practice for patient charts to be placed of the end of a patient's bed so that health care providers can have easy access essential to patient care information. The availability of patient data is important to health care providers but must also be protected from access by unauthorized individuals who are not involved in patient care. HIPAA regulations require that all access to patient records be documented which will change the way that Mary Greeley currently performs internal health care duties.

Creating a logging report system is a major concern of Mary Greeley. Mr. Steffen stated that the area of his organization that is having the most trouble becoming HIPAA

compliant is the logging report system. He also stated that his biggest concern regarding HIPAA compliance infractions is errors in the logging report system. Mr. Steffen's second biggest concern regarding HIPAA infractions is the possibility that a healthcare professional may accidentally release sensitive patient information.

Mr. Steffen commented that there is much confusion among health care professionals as to what can be released and what is prohibited under HIPAA regulations. Mr. Steffen stated that he and other health care providers believe that this confusion is having a negative effect on health care quality within Mary Greeley Hospital.

Mimi Hart, HIPAA Research Analyst for Iowa Health Care Systems, also stated that she believed that HIPAA has had a negative effect on health care quality in regard to the restriction of information that is in the patient's best interest such as nursing home locating.

3.3.2 – External Business Processes

Dennis Potter, Security Coordinator/HIPAA Leader Information Services for Mercy Hospital, stated that he believes identification of external business associates to be one of the most difficult aspects in reaching HIPAA compliance. Mr. Potter also stated that he was concerned that they may never be able to completely identify all external business partners. Mr. Potter stated that he felt that the disclosing of information to business associates was a liability for his organization that is not completely within his control. Mr. Potter, however, did not feel that HIPAA regulations affected negatively on the quality of health care within his organization.

Tom Potts, Manager of Information Protection, and Mimi Hart both agreed that securing compliant business associates would be a daunting task for Methodist Hospital due to each external business partners need to do business with other outside companies that may or may not be compliant.

CHAPTER 4 – COMPARISON OF NATIONAL STATISTICS WITH LOCAL HOSPITALS

4.1 – National Survey

The latest national HIPAA readiness assessment survey was conducted in November of 2002 by the Health Care Information Management Systems Society (HIMSS) / Phoenix Health Systems. The survey was based on 687 health care organizations that responded to the questionnaire. The health care organizations that responded varied is size and function. Here is the break down of the responding health care organizations.

68% of the respondents were health care providers (655), which include:

1. 16% - Hospitals with over 400 beds - 158 respondents
2. 21% Hospitals with between 100 and 400 beds – 205 respondents
3. 12% Hospitals of less than 100 beds
4. 6% Medium sized physician practices/providers (11 to 29 physicians)
5. 12% Small physicians practices/providers (10 or fewer physicians)

The rest of the respondents are:

1. 17% Payers
2. 3% Clearinghouses
3. 12% Vendors

The respondents that this paper is most interested in are the breakout of hospitals with 400+ beds and between 100 and 400 beds. Bruce Hall, the web director for Phoenix Health systems, provided some specific data so that a more direct comparison could be made between national and local hospitals.

4.1.1 - National Survey Results

Table 5. Frequency Data: Various sized hospital participants broken out of the health care providers section courtesy of Bruce M Hall, Web Director for Phoenix Health Systems.

Type of Organization	Number	Percentage
Hospital of 400+ beds	158	16%
Hospital of 100-400 beds	205	21%
Hospital of less than 100 beds	119	12%
Clearinghouse	31	3%
Medium Physician Practice	61	6%
Payer	167	17%
Small Physician Practice	112	12%
Vendor	112	12%

Table 6. Has your organization completed HIPAA transactions and code sets remediation and privacy remediation?

	100 - 400	400+
YES	16%	15%
NO	74%	80%
DON'T KNOW	10%	5%

The majority of national respondents reported that they are not finished with HIPAA transactions and code set remediation and privacy remediation. 74% of the 100 to 400 bed hospitals and 80% of the 400+ bed hospitals reported that they are not finished with the remediation. That number may be higher due to the respondents who are unsure of their current compliance level. All of the local hospitals surveyed reported that they are not finished with HIPAA Transactions and Code Set remediation and Privacy remediation.

Table 7. What HIPAA compliance activities is your organization currently engaged in? (Check all that apply).

100 - 400 beds	T&CS	Unique Ids	Security	Privacy
Awareness/General HIPAA Education	56%	60%	69%	70%
Assessment	53%	38%	66%	59%
Project Planning	66%	30%	52%	68%
Implementation	55%	15%	32%	69%
Training	25%	10%	24%	49%

Over 400 beds	T&CS	Unique Ids	Security	Privacy
Awareness/General HIPAA Education	53%	55%	68%	66%
Assessment	51%	47%	63%	61%
Project Planning	67%	40%	61%	71%
Implementation	59%	22%	40%	77%
Training	24%	2%	23%	51%

The national survey shows that several areas of HIPAA compliance are being addressed simultaneously. Unique Identifiers has scored the lowest among the categories in the implementation phase with security second, transactions and code sets third and privacy scoring the highest. The trend continues for hospitals with 100 to 400 beds and hospitals with 400+ beds.

The local survey lacks the population size to make a complete comparison but it should be noted that both unique identifiers and security sections scored the lowest with 25% in each category. The third most active category for implementation is transactions and code sets with 50% reporting activity in both 100 to 400 and 400+ hospital categories. The most

active category was Privacy with both 100 to 400 and 400+ hospitals reporting 75% implementation efforts. Although the population of local hospitals is small, the trend of implementation activity is similar to national trends.

4.1.2 - National Budget Projections

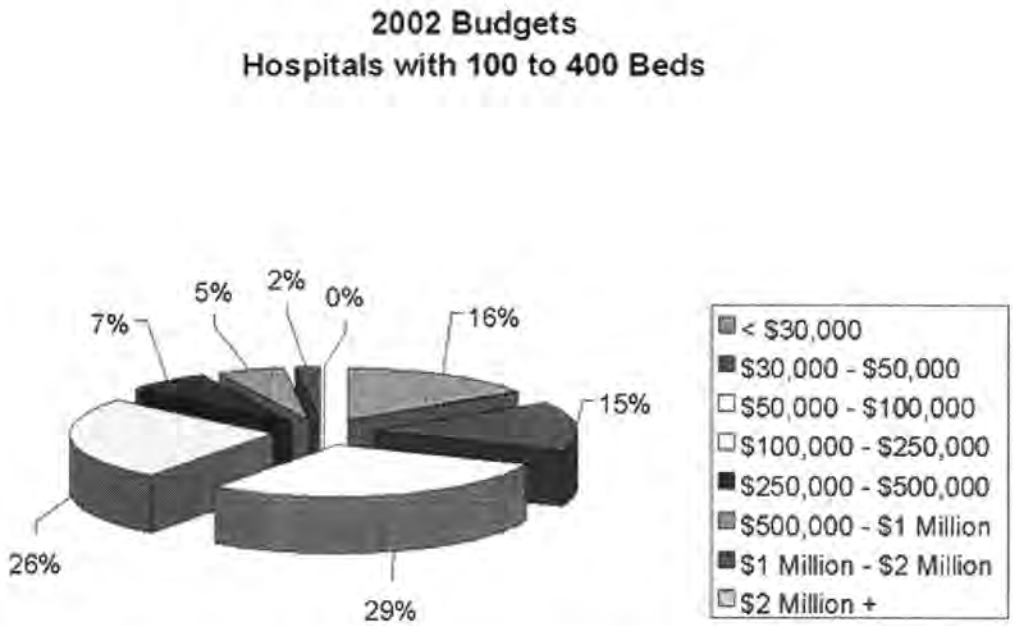


Figure 4. Information gathered from Health Care Information Management Systems Society (HIMSS) / Phoenix Health Systems November 2002 national survey.

The largest group of hospitals with between 100 to 400 beds reported that they believed they would spend between $50,000 and $100,000 on HIPAA compliance efforts the $250,000 to $500,000 and close second. Broadlawns hospital believes that they will spend between $50,000 and $100,000 in 2002, which puts them in the large 29% category nationally. Mary Greeley, however, is in the slimmer 5% national category with their prediction of between $500,000 and $1,000,000 spent in compliance efforts.

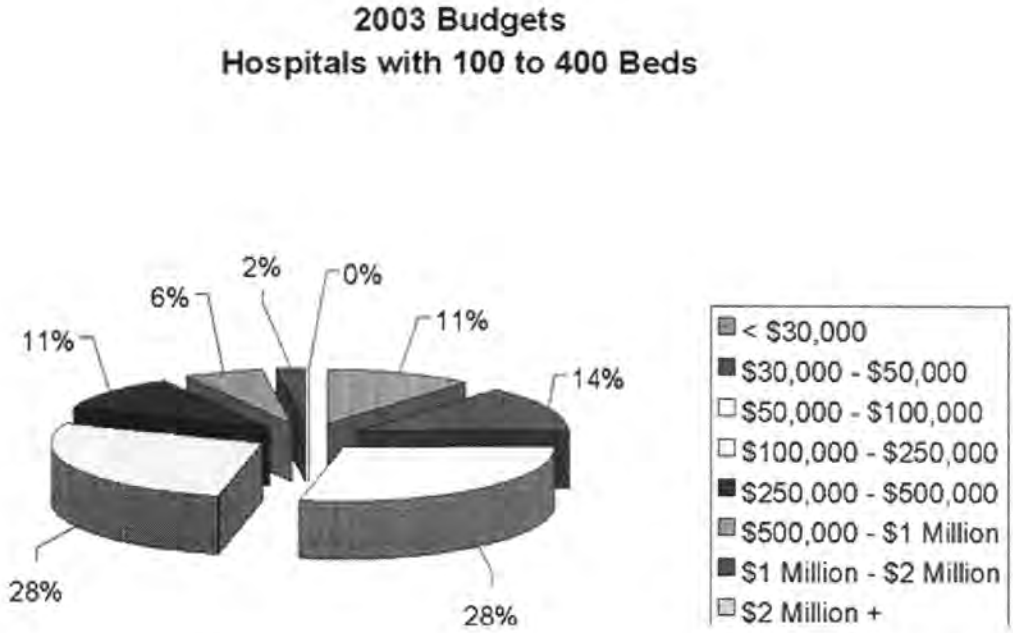


Figure 5. Information gathered from Health Care Information Management Systems Society (HIMSS) / Phoenix Health Systems November 2002 national survey.

Both Broadlawns and Mary Greeley estimate that they will spend between $50,000 and $100,000 during their HIPAA compliance efforts, which puts them within normal national parameters.

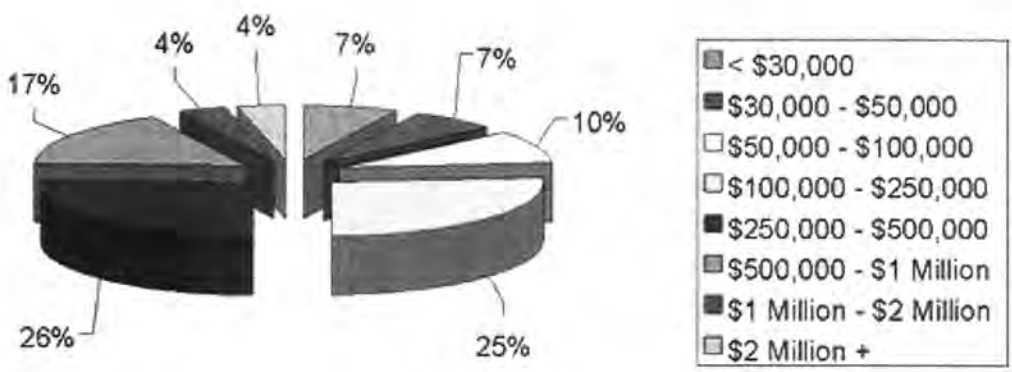


Figure 6. Information gathered from Health Care Information Management Systems Society (HIMSS) / Phoenix Health Systems November 2002 national survey.

Mercy hospital reported that they expect to spend between $100,000 and $250,000 during their efforts to reach HIPAA compliance during 2002. 25% of national respondents reported that they would spend between $100,000 and $250,000 as well putting Mercy's budget estimate within normal national parameters.

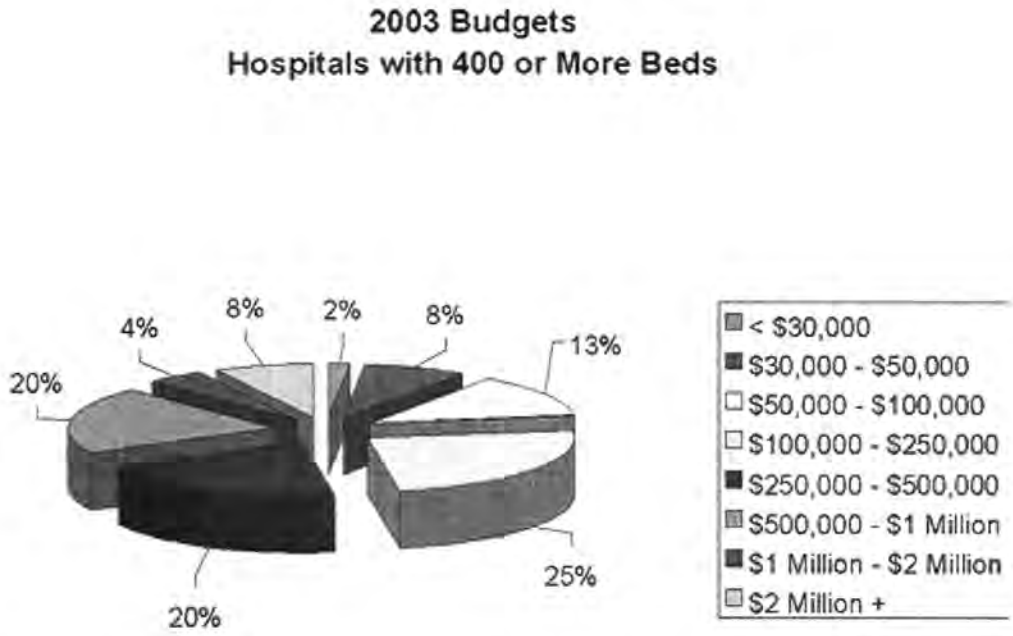


Figure 7. Information gathered from Health Care Information Management Systems Society (HIMSS) / Phoenix Health Systems November 2002 national survey.

Mercy estimated that they would spend between $50,000 and $100,000 during their HIPAA compliance efforts. Only 13% of national respondents reported that they predict to spend between $50,000 and $100,000 during 2003 putting Mercy in the minority nationally but still in the fourth largest section.

CHAPTER 5 – CONCLUSIONS AND FUTURE WORK

The deadline for HIPAA compliance is approaching and local healthcare providers are busy trying to understand HIPAA regulations and implement compliance strategies. An assessment of where healthcare providers currently are with respect to HIPAA compliance is of interest as time begins to run out.

During the comparison it was observed that support for HIPAA among senior management and department heads differed. Two of the surveyed hospitals reported mediocre support from senior management and department heads and one of the surveyed hospitals reported that they believed that HIPAA has outgrown its initial concept and that it should be discontinued. Further research to investigate the effects of poor support from senior management and department heads on HIPAA compliance activity may prove interesting.

Another point of interest discovered during the research was the decision of Mercy and Mary Greeley hospital not to introduce a strategic goal focused on realizing benefits from it's HIPAA compliance efforts. This may indicate that these organizations do not believe that they will benefit from their compliance efforts. Additional research could be pursued to understand if and why healthcare organizations believe that they will not benefit from HIPAA compliance efforts and how many other organization share the feeling. According to the Phoenix Health Systems survey 43% of all polled respondents reported that they, as yet, have not focused on achieving HIPAA benefits from their HIPAA efforts.

Mary Greeley, Broadlawns, Methodist and Mercy hospitals are currently not HIPAA compliant but are not dissimilar from national trends in terms of their compliance level and activity. Budget estimations differed among the locally polled and nationally polled hospitals with the biggest discrepancy coming from Mary Greeley's budget estimation of between $500,000 and $1,000,000 to reach HIPAA compliance spent during the year 2002.

Mary Greeley also reported budget constraints as the second most troublesome roadblock to HIPAA compliance.

Internal and external business processes have been influenced by HIPAA regulations and has been noted by the locally surveyed hospitals. However, perception of the influence varies among the participants as to whether changes, internal and/or external, have a positive or negative effect on quality of health care within each respective organization.

APPENDIX A: LOCAL SURVEY RESULTS – SURVEY 1

Question 1.	Yes	No	Not Sure
Is your organization one or more of the following: -A **Healthcare Plan** -A **Healthcare clearinghouse** -A **Healthcare provider** -An **Employer** whose employees are covered by self funded ERISA Plan	Mercy Methodist Broadlawn Mary Greeley		

Question 2.	Yes	No	Not Sure
Does your organization electronically transmit or exchange health information to carry out financial or administrative activities related to one or more of the following transactions: -Submits claims for healthcare -Provides healthcare payment and remittance advice -Coordination of benefits -Determinations of health claims status -Enrollment and/or disenrollment in a health plan -Eligibility for a health plan -Health plan premium payments -Referral certification and authorization -First report of injury -Health claims attachments -Medical Records transfer, duplication or archival -Other activities involving individually identifiable health information	Mercy Methodist Broadlawn Mary Greeley		

Question 3.	Yes	No	Not Sure
Is your organization a health plan (provides or pays the cost of medical care) with less than 50 employees or receipts of 5 million or less? (If categorized as "small", an additional year is available to meet compliance requirements)		Mercy Methodist Broadlawn Mary Greeley	

Question 4.	Yes	No	Not Sure
Does your organization receive IIHI (individually identifiable healthcare information) from a health plan, healthcare clearinghouse or healthcare provider or from a business associate of one of these entities?	Mercy Methodist Broadlawn Mary Greeley		

Question 5.	Yes	No	Not Sure
Has your organization identified a Privacy Officer (person specifically identified to be in charge of health data privacy)?	Mercy Methodist Broadlawn Mary Greeley		

Question 6.	Yes	No	Not Sure

If your organization is a healthcare plan or healthcare provider, does it give patients a written explanation (notice) of the uses and disclosures of their individually identifiable health information?		Mercy Methodist Broadlawn Mary Greeley	

Question 7.	Yes	No	Not Sure
If you answered Yes to the previous question, have you reviewed your patient notification policies within the last six months?			

Question 8.	Yes	No	Not Sure
If you are a health plan or healthcare provider, does your organization use individually identifiable health information for any of the following uses? Marketing Sell, rent or barter patient information, including mailing lists For health insurance underwriting purposes Disclosure to employers for employment determinations Fundraising	Broadlawn Methodist	Mercy Mary Greeley	

Question 9.	Yes	No	Not Sure
If your organization maintains individually identifiable patient information, does it allow individuals to access their records?	Mercy Methodist Broadlawn Mary Greeley		

Question 10.	Yes	No	Not Sure
If you are a health plan or healthcare provider, do you charge patients for copies of their medical records?	Methodist Broadlawn Mary Greeley		Mercy

Question 11.	Yes	No	Not Sure
Does your organization have written procedures for safeguarding the identity of the patient's (member's) protected health information?	Mercy Methodist Broadlaw Mary Greeley		

Question12.	Yes	No	Not Sure
Has your organization developed policies and procedures to determine the minimum amount of protected health information necessary to accomplish the intended use of the data and if so is there a person designated to make the minimum necessary decision?	Mary Greeley	Mercy Methodist Broadlawns	

Question 13.	Yes	No	Not Sure
If your organization maintains individually identifiable patient information, does it provide		Mercy Methodist	

individuals with an accounting of all disclosures of protected information?		Broadlawn Mary Greeley	

Question 14.	Yes	No	Not Sure
. If your organization is a health plan or healthcare provider, does it enable individuals to amend or correct their medical records?	Mercy Methodist Broadlawn Mary Greeley		

Question 15.	Yes	No	Not Sure
Has your organization appointed someone to be in charge of security?	Mercy Methodist Broadlawn Mary Greeley		

Question 16.	Yes	No	Not Sure
If you answered yes to the previous question, has that person developed an implementation team?	Mercy Methodist Broadlawn		Mary Greeley

Question 17.	Yes	No	Not Sure
Does your organization have written data security policies for workstation use?	Mercy Methodist	Mary Greeley BroadLawn	

Question 18.	Yes	No	Not Sure
If you answered Yes to the previous question, has your organization reviewed these written workstation data security policies within the last 6 months?	Mercy Methodist		

Question 19.	Yes	No	Not Sure
Does your organization have or plan to launch a publicly accessible Web Site?	Mercy Methodist Mary Greeley	Broadlawn	

Question 20.	Yes	No	Not Sure
Does your organization have formal documented policies for granting different levels of access to various types of healthcare information?	Mary Greeley Methodist	Mercy Boadlawn	

Question 21.	Yes	No	Not Sure
If you answered Yes to the previous question, has your organization reviewed its data access policies and procedures in that last six months?	Mary Greeley Methodist		

Question 22.	Yes	No	Not Sure
Does your organization have written policies and procedures for ensuring the physical security of workstation locations?	Mercy Methodist	Broadlawn	Mary Greeley

Question 23.	Yes	No	Not Sure
Does your organization have written personnel	Mercy		

security procedures addressing access to health information?	Methodist Broadlawn Mary Greeley		

Question 24.	Yes	No	Not Sure
Has your organization reviewed its personnel security procedures in the last six months?	Mercy Methodist Mary Greeley	Broadlawn	

Question 25.	Yes	No	Not Sure
Does your organization have and follow policies and procedures in the event of termination of an employee with access to identifiable health information?	Mercy Methodist Broadlawn Mary Greeley		

Question 26.	Yes	No	Not Sure
Does your organization use e-mail to transmit or receive any patient information?	Mercy Broadlawn Mary Greeley	Methodist	

Question 27.	Yes	No	Not Sure
Does your organization allow employees to telecommute?	Mercy Methodist Broadlawn Mary Greeley		

Question 28.	Yes	No	Not Sure
Does your organization have written policies governing the receipt and removal of hardware/software, such as diskettes and tapes, into and out of a facility?	Mary Greeley Methodist	Mercy Broadlawn	

Question 29.	Yes	No	Not Sure
If you answered Yes to the previous question, have you reviewed your policies governing the removal of hardware/software into and out of your facility within the last six months?	Mary Greeley Methodist		

Question 30.	Yes	No	Not Sure
Does your organization have written policies that identify and confirm the identity of a user when he or she tries to access health data?	Mercy Mary Greeley	Broadlawn	Methodist

Question 31.	Yes	No	Not Sure
If you answered Yes to the previous question, has your organization reviewed its written policies that identify and confirm the identity of users within the last six months ?	Mercy Mary Greeley		

Question 32.	Yes	No	Not Sure
Does your organization have specific mechanisms for granting access to protected	Mercy Methodist		

health information on your computer systems and networks?	Broadlawn Mary Greeley		

Question 33.	Yes	No	Not Sure
If your organization uses computer networks or the Internet to transact business, does it have documented procedures, software and hardware that assure the integrity of data, authenticate the message and verify the identity of the sender and recipient?	Mary Greeley	Broadlawn Mercy	Methodist

Question 34.	Yes	No	Not Sure
If you answered Yes to the previous question, has your organization evaluated the effectiveness of its systems that assure data integrity, authenticate the message and verify the identity of the sender and recipient within the last six months?	Mary Greeley		

Question 35.	Yes	No	Not Sure
Does your organization use open networks to transmit or receive health data?	Mercy Methodist Mary Greeley	Broadlawn	

Question 36.	Yes	No	Not Sure
Does your organization have specific mechanisms for authenticating the sender and recipient of electronically transmitted data?	Mary Greeley Mercy	Broadlawn	Methodist

Question 37.	Yes	No	Not Sure
Does your organization use or plan to use digital signatures within the next 12 months?	Methodist Broadlawn Mary Greeley	Mercy	

Question 38. Does your organization have written procedures for reporting and responding to computer security breaches?	Yes	No	Not Sure
	Mercy Methodist Mary Greeley	Broadlawn	

Question 39.	Yes	No	Not Sure
If you answered Yes to the previous question, has your organization reviewed its breach of security procedures in the last six months?	Mary Greeley Methodist	Mercy	

Question 40.	Yes	No	Not Sure
Does your organization plan to have an evaluation of your security system and/or confidentiality practices performed by an outside entity within the next 12 months?	Broadlawn Methodist	Mary Greeley Mercy	

Question 41.	Yes	No	Not Sure
In the last 12 months, has your organization conducted a comprehensive risk assessment of its vulnerability to a security breach?	Methodist Broadlawn Mary Greeley		Mercy

Question 42.	Yes	No	Not Sure
Has your organization filed for an extension for the Transactions and Code Sets deadline?	Mercy Methodist Broadlawn Mary Greeley		

Question 43.	Yes	No	Not Sure
Do you have a written detailed disaster and contingency plan to respond to computer system emergencies?	Mercy Methodist Broadlawn Mary Greeley		

Question 44.	Yes	No	Not Sure
If you answered Yes to the previous question, has your organization reviewed its contingency plans within the last six months?	Mercy Methodist Broadlawn Mary Greeley		

Question 45.	Yes	No	Not Sure
Does your organization have a comprehensive computer security training program for all employees?	Mary Greeley	Mercy Broadlawn	Methodist

Question 46.	Yes	No	Not Sure
Has your organization conducted security awareness training in the last six months?		Mercy Broadlawn Mary Greeley	Methodist

Question 47.	Yes	No	Not Sure
Has your organization provided training to its employees, agents and contractors regarding the confidentiality of health information?	Mary Greeley Broadlawn	Mercy	Methodist

Question 48.	Yes	No	Not Sure
Has your organization budgeted any resources to provide for HIPAA compliance?	Mercy Methodist Broadlawn	Mary Greeley	

Question 49.	Yes	No	Not Sure
If you answered No to the previous question, does your organization plan to add HIPAA compliance, training and education to the new budgetary cycle?	Mary Greeley		

Question 50.	Yes	No	Not Sure

Does your organization plan to handle HIPAA compliance internally?	Mercy Broadlawn Mary Greeley	Methodist	

Question 51.	Yes	No	Not Sure
Does your organization establish or terminate insurance coverage by transmitting subscriber enrollment information to a health plan?	Methodist Mercy	Mary Greeley Broadlawn	

Question 52.	Yes	No	Not Sure
If your organization is a health care provider or health plan, does it transmit **Remittance Advice** and/or **Explanation of Benefits**?	Mercy Broadlawn	Mary Greeley Methodist	

Question 53.	Yes	No	Not Sure
Does your organization transmit encounter data for reporting purposes, internally or between providers and plans (even though services are prospectively paid by capitation or other methods?	Methodist	Mercy Broadlawn Mary Greeley	

Question 54.	Yes	No	Not Sure
Does your organization transmit claim requests, or respond to claim requests for payments and accompanying information either internally or externally?	Mercy Methodist Broadlawn Mary Greeley		

Question 55.	Yes	No	Not Sure
Does your organization transmit or receive authorizations for health care or referral authorizations?	Mercy Methodist Broadlawn Mary Greeley		

Question 56.	Yes	No	Not Sure
Does your organization inquire or respond to inquiries regarding the status of a health care claim?	Mercy Methodist Broadlawn Mary Greeley		

Question 57.	Yes	No	Not Sure
Does your organization use an outside vendor's system for the collection, dissemination, transfer and archival of individually identifiable health information?	Methodist Broadlawn Mary Greeley	Mercy	

Question 58.	Yes	No	Not Sure
If you answered Yes to the previous question, what is the vendors time line for HIPAA compliance?	Mary Greeley Methodist		Broadlawn

Question 59.	Yes	No	Not Sure
If you answered Yes to #57, has HIPAA compliance been addressed contractually with your vendor?	Mary Greeley Methodist		Broadlawn

Question 60.	Yes	No	Not Sure
Has your organization reviewed its contracts with health plans, healthcare clearinghouses, healthcare providers and/or employers from a HIPAA compliance standpoint?	Methodist	Mercy	Mary Greeley Broadlawn

APPENDIX B: LOCAL SURVEY RESULTS – SURVEY 2

Question 1.	Not Started	Planning	In Progress	Finished
Has your organization determined executive fiscal responsibility for HIPAA compliance fulfillment?				Mercy Methodist Broadlawns Mary Greeley

Question 2.	Not Started	Planning	In Progress	Finished
Has your organization appointed a team of appropriate people to undertake the hands-on responsibilities required for remediation with HIPAA's requirements?			Mary Greeley Broadlawn	Mercy Methodist

Question 3.	Not Started	Planning	In Progress	Finished
Have you established and conducted an organization-wide HIPAA Compliance Awareness training program?			Mercy Broadlawn Mary Greeley	Methodist

Question 4.	Not Started	Planning	In Progress	Finished
Has research been conducted and completed to determine which State laws governing your organization will preempt HIPAA regulations?			Mercy Methodist Broadlawn Mary Greeley	

Question 5.	Not Started	Planning	In Progress	Finished
Have you planned, conducted and completed organization-wide initial readiness assessments, gap analyses, and risk analyses for determining the best plan of action for complete organizational compliance with HIPAA mandates?			Methodist Mary Greeley	Mercy Broadlawn

Question 6.	Not Started	Planning	In Progress	Finished
Have you compiled a complete inventory of all information systems, data flow processes between persons or entities, all policies & procedures, and all business associate agreements, and defined all actions needed to bring each item into compliance with HIPAA mandates?		Mary Greeley	Mercy Methodist	Broadlawn

Question 7.	Not Started	Planning	In Progress	Finished
Have project plans been created and finalized for each separately identified HIPAA action project, and has an implementation schedule been established			Mercy Methodist Mary Greeley	Broadlawn

to prioritize each of these projects?				

Question 8.	Not Started	Planning	In Progress	Finished
Have each of these projects been completed, implemented, tested, and finalized? Please comment below. – Mercy did not answer			Methodist Broadlawn Mary Greeley	

Standard Identifier Questions

Question 1.	Not Started	Planning	In Progress	Finished
Have you reviewed and addressed all duplication errors contained in your Master Patient Index?		Mercy Methodist Broadlawn Mary Greeley		

Question 2.	Not Started	Planning	In Progress	Finished
Have you integrated your assigned National Provider Identifier for each area within your organization required to have one, and verified each with all payers your organization works with, as well as all medical provider associates?	Mercy Methodist Broadlawn Mary Greeley	Mercy		

Electronic Transactions and Code Sets Questions

Question 1.	Not Started	Planning	In Progress	Finished
Have steps been taken to revise or replace existing automated systems to ensure that all HIPAA covered electronic transactions conducted by your organization are sent using the proper ANS ASC X12N standards as required?			Mercy Methodist Broadlawn Mary Greeley	

Question 2.	Not Started	Planning	In Progress	Finished
Has a cost benefit analysis been conducted and reviewed to evaluate the use of an in-house solution for transaction processing as compared to a clearinghouse solution?			Methodist Mary Greeley	Mercy Broadlawn

Question 3.	Not Started	Planning	In Progress	Finished
Have all code sets currently in use by your organization been reviewed and determined to be consistent with HIPAA requirements?			Methodist Broadlawn Mary Greeley	Mercy

Question 4.	Not Started	Planning	In Progress	Finished
Have appropriate mechanisms been developed and implemented to effectively monitor your organization's compliance		Mercy	Methodist	Mary Greeley Broadlawn

with official coding guidelines?				

Question 5.	Not Started	Planning	In Progress	Finished
Have you developed a plan for, implemented, and documented regular training sessions for your coding staff on current coding practices as required by HIPAA?	Methodist Mercy		Mary Greeley Broadlawn	

Privacy Questions

Question 1.	Not Started	Planning	In Progress	Finished
Have HIPAA compliant policies and procedures for safeguarding the access to information contained in the patient's paper-based, as well as electronic health record been developed and implemented?			Mercy Methodist Broadlawn Mary Greeley	

Question 2.	Not Started	Planning	In Progress	Finished
Have HIPAA required processes for documenting the ALL disclosures of protected patient health information been developed and implemented?			Mercy Methodist Broadlawn Mary Greeley	

Question 3.	Not Started	Planning	In Progress	Finished
Have HIPAA required "minimum necessary" requirements for disclosure of information been determined and implemented for each person or entity sharing electronic, personally identifiable health information?			Mercy Methodist Broadlawn Mary Greeley	

Question 4.	Not Started	Planning	In Progress	Finished
Have policies and procedures been developed and implemented to provide the protection HIPAA requires for all data, including financial, that may contain elements of individually identifiable information?			Mercy Methodist Broadlawn Mary Greeley	

Question 5.	Not Started	Planning	In Progress	Finished
Have protective Business Associate & Trading Partner Agreements been conceptualized, written and signed to restrict all qualified entities' disclosure of protected health information?			Mercy Methodist Broadlawn Mary Greeley	

Question 6.	Not Started	Planning	In Progress	Finished

Have appropriate policies and procedures concerning appropriate patient education, including privacy policies and grievance procedures, medical consent forms, and release of information forms been developed and implemented?			Mercy Methodist Broadlawn Mary Greeley	

Question 7.	Not Started	Planning	In Progress	Finished
Has a comprehensive, HIPAA compliant, Health Information Privacy and Confidentiality Training Program, including responsibilities and penalties for non-compliance, been developed and implemented for all employees and staff members?			Mercy Methodist Broadlawn Mary Greeley	

Security Questions

Question 1.	Not Started	Planning	In Progress	Finished
Have you developed and implemented HIPAA Compliant policies and procedures to cover ALL areas of your organization's data and physical security?			Mercy Methodist Broadlawn Mary Greeley	

Question 2.	Not Started	Planning	In Progress	Finished
Have procedures been developed and put into place to individually identify and authenticate each information system user, require logoff if work station is left idle, and maintain audit trails as required by HIPAA?		Mary Greeley	Mercy Methodist Broadlawn	

Question 3.	Not Started	Planning	In Progress	Finished
Have you developed and implemented HIPAA compliant policies and procedures to require the control of, ongoing monitoring of, and documentation of unauthorized access to individually identifiable health information?			Mercy Methodist Broadlawn Mary Greeley	

Question 4.	Not Started	Planning	In Progress	Finished
Have you created and implemented policies and procedures to require and direct the review of potential employees using appropriate screenings and background checks?		Methodist	Mary Greeley	Mercy Broadlawn

Question 5.	Not Started	Planning	In Progress	Finished
Has the overall security of each of your automated systems rooms been fully tested and documented?		Mary Greeley	Methodist	Mercy Broadlawn

Question 6.	Not Started	Planning	In Progress	Finished
Have HIPAA required encryption and authentication procedures been put in place to protect all covered, electronically available health data?		Mercy Methodist Mary Greeley	Broadlawn	

Question 7.	Not Started	Planning	In Progress	Finished
Have HIPAA compliant policies and procedures been developed and reviewed, approved, and implemented to accommodate appropriate data back-up and complete disaster recovery procedures?		Mary Greeley	Methodist Mercy	Broadlawn

Question 8.	Not Started	Planning	In Progress	Finished
Overall, how far do you consider your organization to have progressed towards completion of its HIPAA Compliance Implementation Project?			Mercy Methodist Broadlawn Mary Greeley	

APPENDIX C: LOCAL SURVEY RESULTS – INTERVIEW SURVEY

1. What do you think are your strong areas in regard to HIPAA compliance?
    a. Mercy-Transactions and Code Sets
    b. Methodist – HIPAA steering committee
    c. Mary Greeley – Knowledgeable staff
2. How much money do you think has been spent thus far in trying to become HIPAA compliant?
    a. Mercy – 400,000 to 500,000 so far not including labor
    b. Methodist – 100,000 to 500,000 mostly labor.
    c. Mary Greeley – 60 to 70 thousand – new system coming in.
3. How many new people have been hired thus far as a result of HIPAA regulations?
    a. Mercy - 0
    b. Methodist – 1 outside consultant – may hire more to perform testing
    c. Mary Greeley - 0

4. How many people do you think you will need to hire by the time HIPAA compliance must be reached?
    a. Mercy - 0
    b. Methodist – No full time staff
    c. Mary Greeley - 0

5. What is the most difficult part of HIPAA compliance/implementation?
    a. Mercy – Training and identification of business assoc. may not be able to completely identify all business associates
    b. Methodist – Human Nature "changing peoples ideas and behaviors".
    c. Mary Greeley – Trying to understand and keep up with regulations.

6. What if anything would you change about HIPAA that would make is easier to implement?
    a. Mercy – State law preemption.
    b. Methodist – released privacy and security rules at same time.
    c. Mary Greeley – Get rid of HIPAA all together. Politicians don't know what they are doing. HIPAA regulations will increase paper work. It has become something that it initially was not intended to be.

7. What area/dept. is having the most trouble reaching HIPAA compliance?
    a. Mercy – Nursing, doctors, staff – direct patient care personnel.
    b. Methodist – People who are used to easy access to patient information.
    c. Mary Greeley – Logging report – releasing information record.

8. What area/dept. is least accepting of the HIPAA regulations? Why?
    a. Mercy – IT department
    b. Methodist – Physicians
    c. Mary Greeley - Physicians

9. Do you think that you will ever feel comfortable with your organizations compliance with HIPAA requirements?
    a. Mercy – Yes -
    b. Methodist - Yes
    c. Mary Greeley - Yes

10. What are your largest areas of concern regarding HIPAA compliance with respect to possible fines?
    a. Mercy – Not logging off workstations
    b. Methodist – Disgruntled employee may complain
    c. Mary Greeley – Log report errors – health care professionals accidentally release patient info. There is a lot of confusion about what can and cannot be released.

11. Are there areas that you feel are out of your control regarding patient record safety in which you are still accountable?
    a. Mercy – Disclosing information to business associates is a liability
    b. Methodist – Controlling the emailing of patient information challenging.
    c. Mary Greeley – Physical control of patient chart

12. In case of a breach of security do you feel that you would be able to prove that you used best practice methods to secure the compromised data?
    a. Mercy - Yes
    b. Methodist - Yes
    c. Mary Greeley - yes

13. How much money/people/time will you have to commit to prove you are using best practice methods, with respect to HIPAA, to avoid paying a hefty fine in the case of patient record compromise?
    a. Mercy – Not much – proving compliance is covered in becoming compliant.
    b. Methodist – Too early to tell – need more info about security requirements.
    c. Mary Greeley - Logging

14. Where, so far is the most money being spent attempting to reach compliance?
    a. Mercy – Disaster recovery and data backups
    b. Methodist - EDI
    c. Mary Greeley – Privacy Officer and director time planning "reading the forms".

15. Where do you think most of the money will be spent after compliance has been reached?
    a. Mercy – Training - Training has to be done after hours – most employee's are hourly which means overtime.
    b. Methodist - Security
    c. Mary Greeley – Staff training – releasing patient information person.

16. Where do you think most of the money will be spent during maintenance of HIPAA compliance?
    a. Mercy – Ongoing training – constant training, usually 200 to 250 open positions at mercy at any given time.
    b. Methodist - Security
    c. Mary Greeley – Setting up logging system

17. Do you of any one else in your organization feel that HIPAA will have a negative impact in some areas of health care quality? If so who and in what areas?
    a. Mercy – No. No negative impact.
    b. Methodist – Yes. Requirements of authorization limits free flow of information that is in the patients best interests such as nursing home locating.
    c. Mary Greeley – Yes – Not knowing what information can be released.

18. Have you thought about outside consultants?
        - if an employee of an outside consultant whom worked on you organizations information system is fired how will you be protected from such a person?
    b. Mercy – No and no plans to do so.
    c. Methodist – Yes – consider consultant access methods to the network and sign non-disclosure agreement. "initial thought to access control given to outside consultants and vendors."
    d. Mary Greeley – No. Too pricey.

19. What is you assessment of your current security and privacy standards? – Secure, fairly secure, insecure?
        - Compare above question with standard best practice methods and best practice methods with respect to HIPAA regulations.
    b. Mercy – Fairly secure – Feel 50 to 60% secure in regard to both HIPAA and Industry standard best practice methods.
    c. Methodist – Security - In between fairly secure and secure – Privacy fairly secure – ambulance need billing information face sheet has more info on it then needed. Also feel business assoc. will be a daunting task due to each business' need to do business with other companies. We need to weed out the people.
    d. Mary Greeley – Fairly secure – Created big confusion problem with regard to privacy believes HIPAA is out of realm.

Additional Comments

Mary Greeley

Interview with Shawn Steffen, Director of the Business Office, Medical Records.
Currently patient charts are kept at the foot of the patient's bed allowing health care professionals easy access to patient information. We will probably have to go to a electronic patient chart to continue to allow easy access to patient information and also be able to log and control access.

APPENDIX D: NATIONAL SURVEY RESULTS

HIMSS / Phoenix Health Systems

U.S. Healthcare Industry Quarterly HIPAA Survey Results: Fall 2002

EXECUTIVE OVERVIEW

As our Fall Survey polling period closed in mid-October, healthcare organizations impacted by HIPAA regulations were just six months away from two important deadlines: the Privacy compliance deadline and the deadline to begin transactions testing. Despite earlier hopes of many covered entities, progress toward these deadlines has been slow, reportedly still hampered by regulatory interpretation difficulties, cost issues and poor communications between trading partners. Some significant trends noted in the Fall Survey include:

- HIPAA support from senior officers, initially difficult to achieve, remains generally strong.
- The healthcare industry is moving slowly towards achieving compliance. Survey results showed little progress since the Summer 2002 Survey conducted in early July, with fewer than 50% of respondents having completed their gap assessments. Worse, only 5% of providers and payers had actually completed Privacy and Transactions remediation.
- Major roadblocks to HIPAA compliance include "interpretation of the regulations" and "not enough time." Cost concerns, issues of state preemption and a lack of industry "best practices" are increasingly being cited.
- Over 80% of all respondents applied for the Transactions deadline extension from October 2002 to October 2003.
- Covered entities are focusing mainly on Privacy and Transactions compliance; Security initiatives are moving more slowly, despite Privacy Rule mandates for strong security measures to protect confidentiality.
- Across the industry, HIPAA budgets are generally higher for 2003 than for 2002.

THE SURVEY

Phoenix Health Systems and HIMSS conducted the Fall 2002 U.S. Healthcare Industry Quarterly HIPAA Compliance Survey early in October. Following e-mail appeals to HIMSS 12,000+ members and to Phoenix' 19,000+ HIPAAlert newsletter subscribers, a record total of 965 healthcare industry representatives responded, an increase of 40% over last quarter's response. The online survey was completed anonymously via Phoenix' website HIPAAdvisory.com.

The Organizations

Respondents from provider organizations accounted for 68% (655) of participants. The breakout of participants follows:

- Providers - 68%
  - Hospitals of 400+ beds: 16%
  - Hospitals of 100-400 beds: 21%
  - Hospitals of less than 100 beds: 12%
  - Medium-sized physician practices (11 to 29 physicians)/other providers: 6%
  - Small physicians practices (10 or fewer physicians)/other providers: 12%
- Payers - 17%
- Clearinghouses - 3%
- Vendors - 12%

Within the Organizations

A total of 87% of all respondents have an "official" role within their organization for HIPAA compliance. The majority of respondents hold management or executive level positions, including 17% at Senior Management level, and another 11% who function as the Chief Information Officer. The largest group of respondents (28%) works specifically in the compliance/security arena. Executive support for HIPAA compliance efforts remains generally high with about 60% of respondents reporting that their senior management is providing moderately strong to strong support.

THE BIG QUESTION...

Has your organization completed HIPAA Transactions and Code Sets(TCS) remediation AND Privacy remediation?
The great majority of respondents answered "No." More specifically, 95% of providers and payers reported they had not completed these efforts; 5% have. Vendors appeared to be much farther along, with 38% reporting that they had completed Transactions remediation and 19% Privacy remediation. 13% of clearinghouse respondents reported that their Transactions remediation was complete, though only 6% had finished Privacy implementations.

THE BIG HURDLES

Participants who reported that they had completed Transactions and Code Sets and Privacy remediation identified "understanding/interpreting the legal requirements" (101 of 162 respondents) as the most difficult aspect of the HIPAA remediation process. However, "resolving issues with third parties" was a very close second. Survey participants called for increased cooperation among all industry sectors. The following is a sampling of comments:
Medium-size Physician Practice

- "We feel we are on track with those elements of compliance which are within our control. Full compliance in those areas will occur within the month. Too many parameters (software, clearinghouse) are not within our control...communication has been poor to non-existent."
- "Our clearinghouse is ready but very few of the payers have even begun testing with them."

Vendor

- "I've noticed that our clients are FINALLY waking up to the reality of HIPAA and are purchasing software and planning on testing. Most will barely make the cutoff."

Clearinghouse

- "[We are] actively sending HIPAA compliant transactions to several payers. However, many payers have filed extensions and are not even ready to begin the testing process. This has been the hold-up in our HIPAA compliance efforts."

Provider representatives, most of whom had not completed remediation efforts, rank-ordered several factors as impediments to HIPAA compliance. "Interpretation of the regulations" and "not enough time" were ranked first as the biggest roadblocks, followed by "budget constraints" (the same three major impediments reported in recent past surveys). Written comments by respondents brought focus to other areas of difficulty - state law pre-emption and a general dearth of "best practices" guidance.

- "Interpretation is a key issue...but...not the biggest roadblock. If we, as a struggling hospital were able to get external, full-time, knowledgeable and proven assistance (i.e., expensive assistance) with compliance efforts, all of us would feel better about the regs. Therefore, budget constraints (because it keeps us from bringing in external help) and time (juggling numerous duties along with HIPAA) are the biggest problems...."
- "Privacy regulations are much more difficult to understand and interpret...We should as an industry be able to come together and share and leverage what we have learned. 'Benchmarks Best Practices' is a warranted industry need."
- "There are very few 'experts' available to help decipher the new regulations and very few documented 'best practices' to aid in deciding how to address certain situations."
- "The people working on the HIPAA team already wear so many different hats in the organization that it's hard to commit "enough time" to work on the project."
- "Pre-emption analysis is also trying -- state rules and 42 CFR affect how HIPAA impacts us."

IMPACT OF FINAL PRIVACY RULE MODIFICATIONS

As of August 14, 2002, the Department of Health and Human Services finalized modifications to the Privacy Rule. Respondents were asked how integrating the modifications into ongoing compliance efforts would affect overall progress. Over half (57%) of both provider respondents and total respondents said that the proposed Privacy Rule modifications will have no effect on their compliance progress. A smaller percentage (38%) indicated that their progress would slow, while only 4% predicted that they would now miss the deadline for privacy compliance.

IMPACT OF TRANSACTIONS EXTENSION

By the close of the survey period (October 14) 80% of respondents indicated that they had applied for the Transactions compliance deadline extension offered in the Administrative Simplification Compliance Act, up from 27% in Summer 2002. Another 10% noted that they expected to apply before the application deadline of October 15. Only 4% of respondents indicated that they would be in compliance by the original October 2002 compliance deadline.

Which Transactions Version?

Reports for both Fall and Summer 2002 indicated that over 60% of respondents are implementing the HIPAA transactions published in May 2000, as opposed to those published in the recent Transactions

NPRM. However, it should be noted that many respondents, 35% of 965, do not know which transactions they will implement.

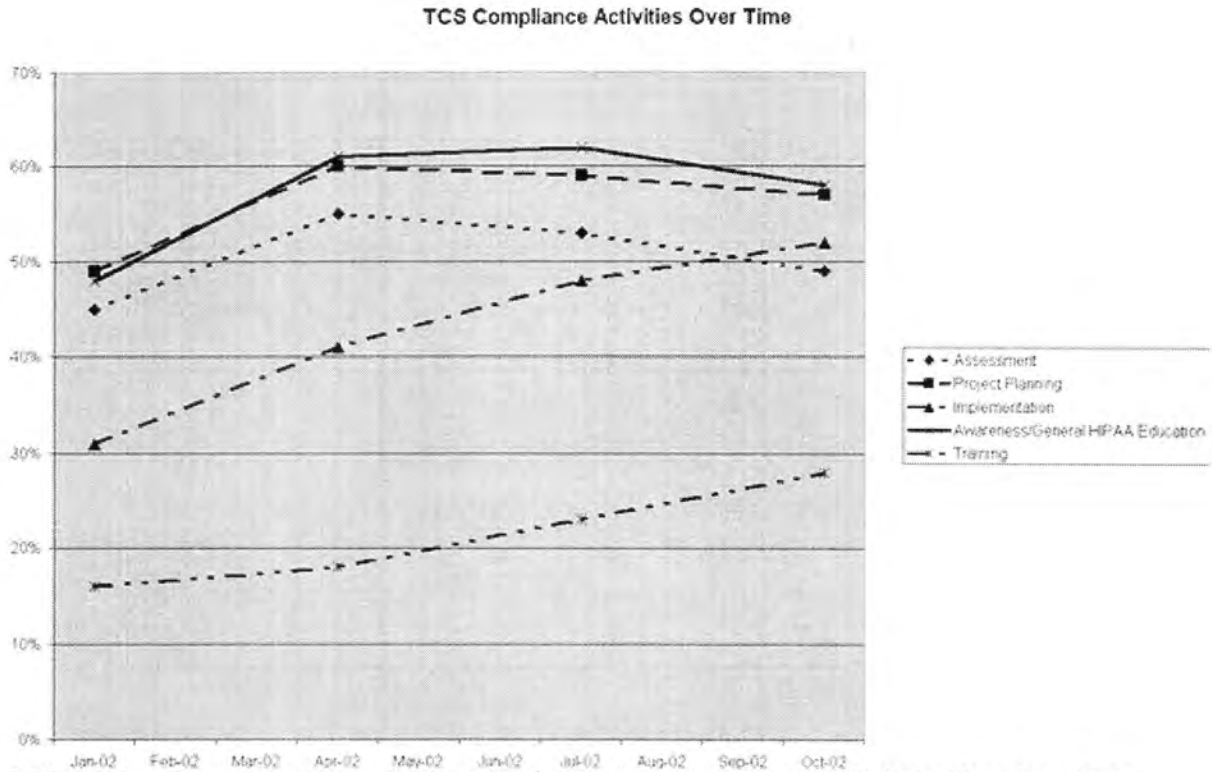
FOCUS OF ENTERPRISE HIPAA EFFORTS

Compliance Approach

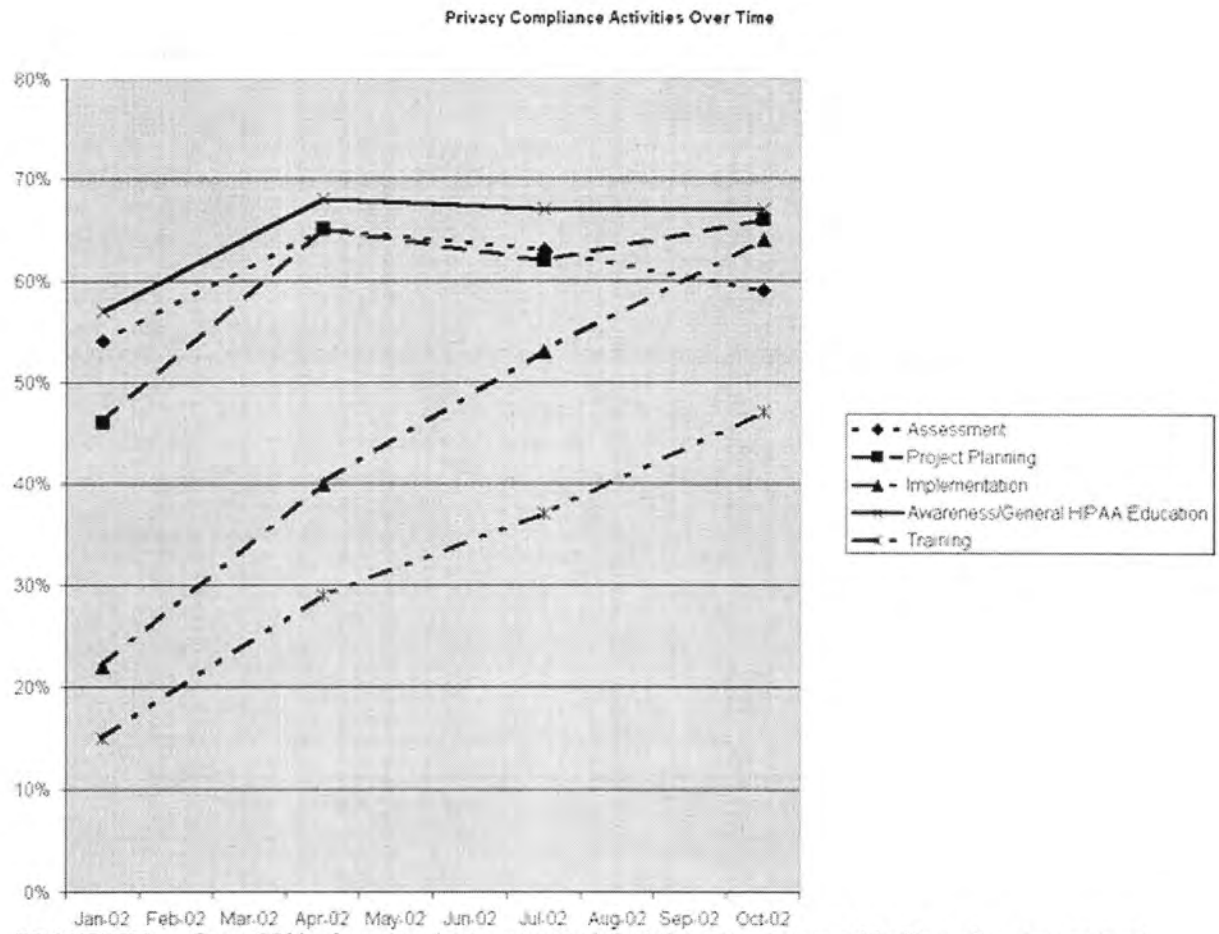
Readers will welcome the news that, among payers, the implementation trend may be gradually shifting from working alone (44%, down from 50% in Summer 2002) to coordinating more directly with providers (41%, up from 37% in Summer 2002). Providers agree that there is more interaction with payers, although only 31% of providers reported that their payers were either moderately or very forthcoming in providing information. Providers appear more satisfied with vendor communications related to HIPAA; nearly 60% reported that their vendors are moderately or very communicative. More payers (57%) are focusing on remediation of existing software rather than on the development of new software (35%), with some working on both. The number of respondents planning to use the clearinghouse option to provide front-end remediation has increased from 27% to 32%.
Most clearinghouse participants are focusing first on internal software remediation, then on internal new software development.

Current Compliance Activity by Phase

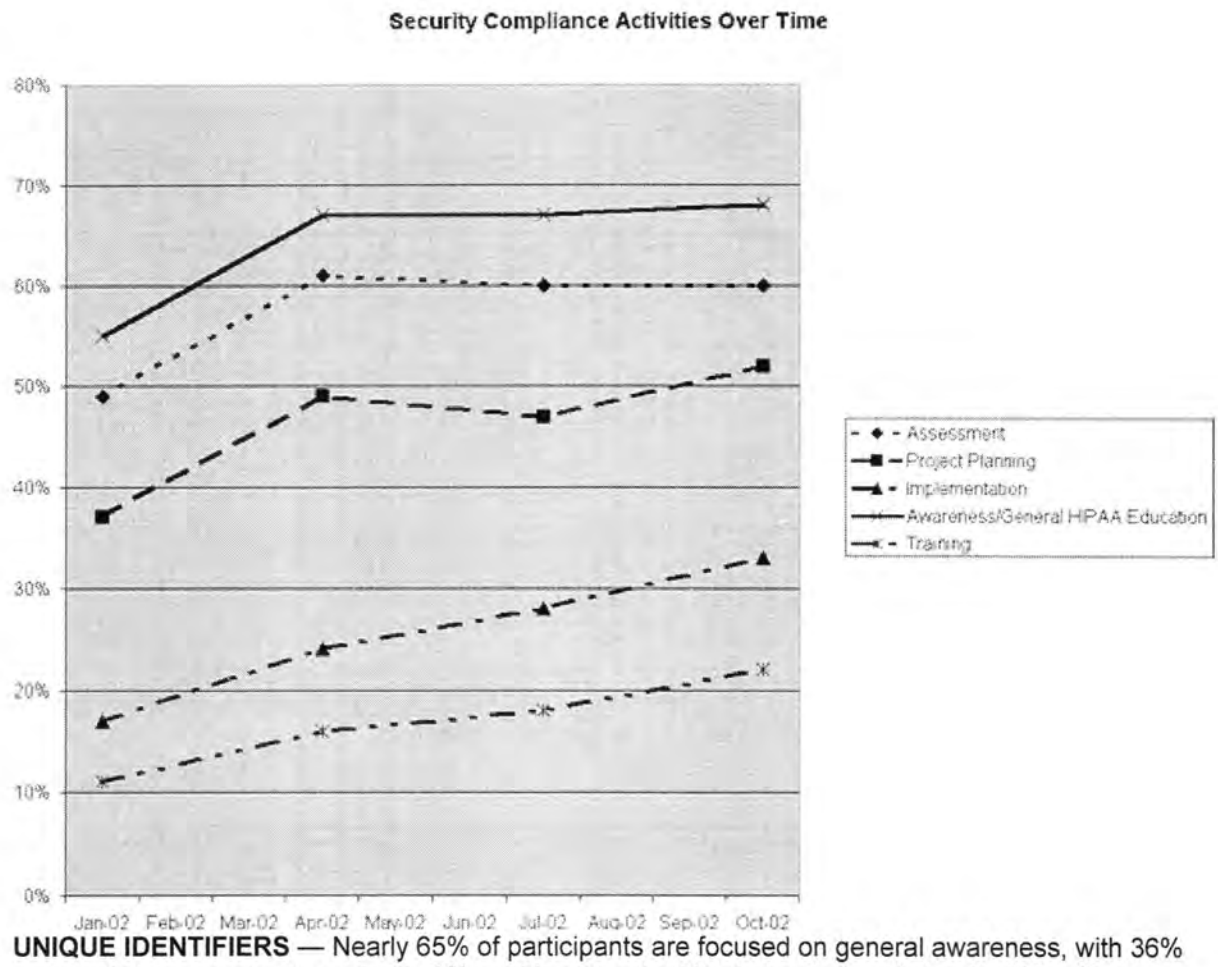
OVERALL HIPAA AWARENESS — Across all industry segments, HIPAA awareness and education continue to be a primary focus of ongoing compliance activity in all major compliance areas. Among all industry segments, organizations reportedly are involved in HIPAA awareness and education activities as follows: Transactions - 58%, Security - 68%, Privacy - 67% and Unique Identifiers - 60%.
TRANSACTIONS AND CODE SETS — Compliance activities focusing on Transactions and Code Sets generally have moved beyond assessment into project planning and implementation phases. With some overlap, 57% of respondents are doing project planning and 52% (up from 48% in Summer 2002) are in the implementation phase. By industry segment: 46% of providers, 55% of vendors, 68% of payers, and 77% of clearinghouses are engaged in transactions implementation initiatives.



PRIVACY — Respondent organizations are focused most on Privacy initiatives. Results reflect a gradual move past the assessment phase, as evidenced by the increase in organizations focusing on project planning - 66% (up from 62% in Summer 2002) and implementation - 64% of all participants (up from 53%). Privacy accounts for most of training activity - 47% (up from 37%).



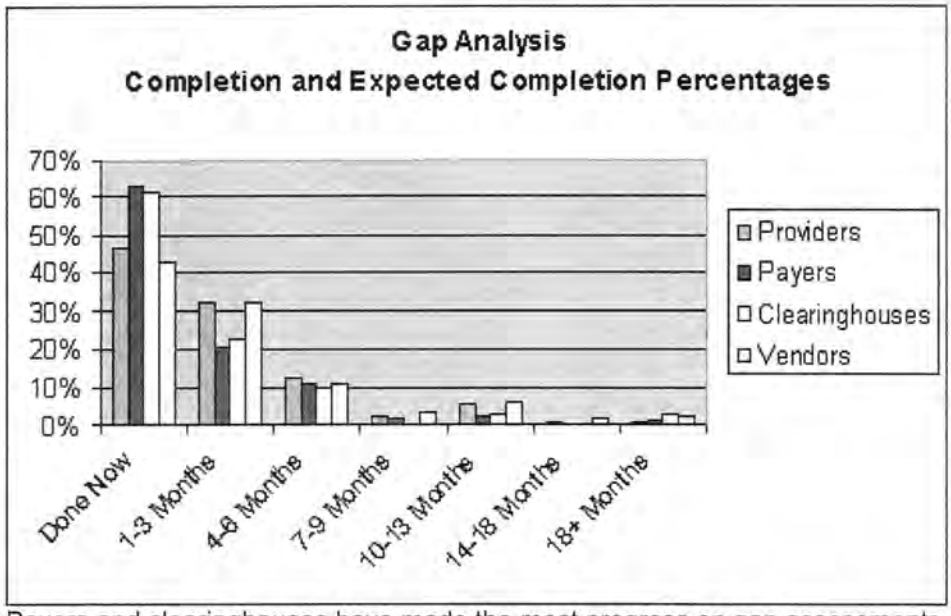
SECURITY — Over 60% of respondents reported that they are engaged in Security assessment activities. Activity is gradually increasing in the Security implementation phase (33%, up from 30% in the Summer 2002 Survey, and 24% in the Spring 2002 Survey).



UNIQUE IDENTIFIERS — Nearly 65% of participants are focused on general awareness, with 36% engaged in assessments, and only 8% working on actual implementation of standard identifiers.

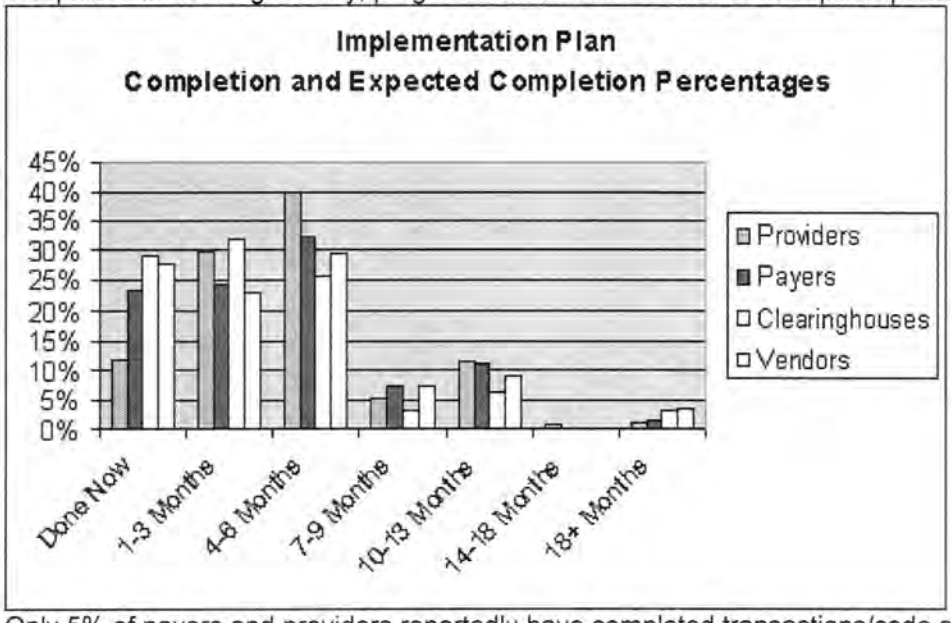
Industry HIPAA Compliance Progress

The survey questioned providers, payers, clearinghouses and vendors about their organizations' real-time progress in HIPAA remediation, and when they would be ready to use HIPAA transactions. Across the industry, less than 50% of respondents had completed gap assessments by early October, indicating slow progress in the last three months. About 40% had finished assessments as of our Summer 2002 Survey, and another 30% of our Summer respondents planned to be finished by now, but most had not done so. Again, another 30% plan to complete assessments within three months.

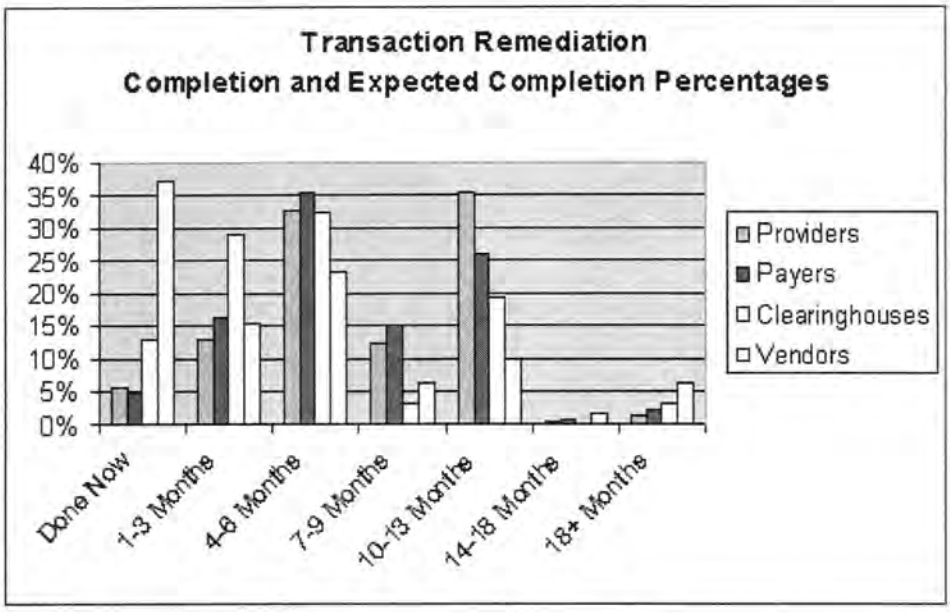


Payers and clearinghouses have made the most progress on gap assessments, with over 60% having completed them. About 45% of providers have finished assessments; however, hospitals in all groups, except those with less than 100 beds, have made significantly more progress (about 59% have completed assessments) than smaller providers (only 34% of hospitals with less than 100 beds, and even fewer smaller provider organizations have finished assessments).

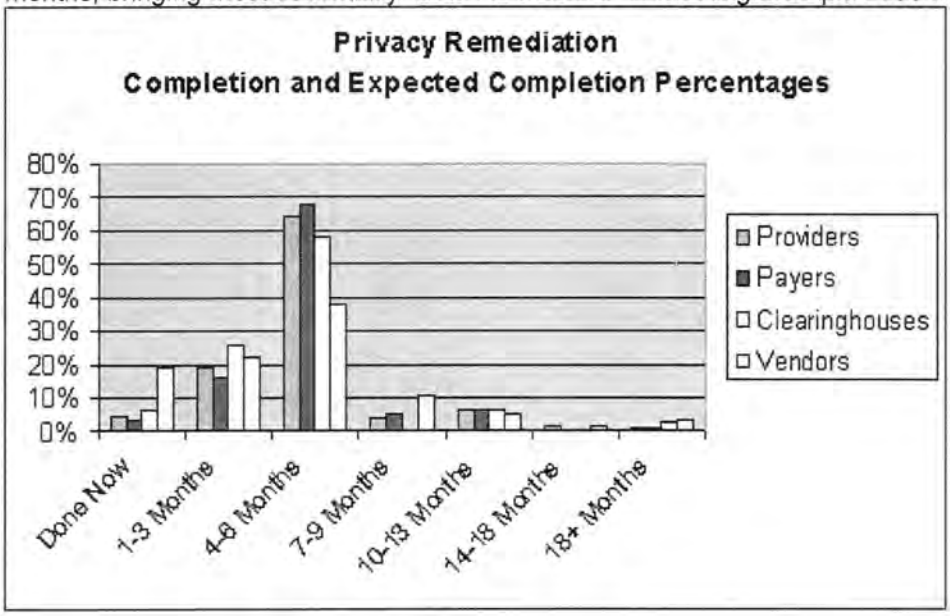
When asked about plans to finalize a HIPAA remediation implementation plan, the majority of respondents said that their plans would be finished within six months, again not unlike the expectations reported in our Spring and Summer 2002 Survey reports. So, while numbers for completion increase gradually, progress has been much slower than participants had anticipated.



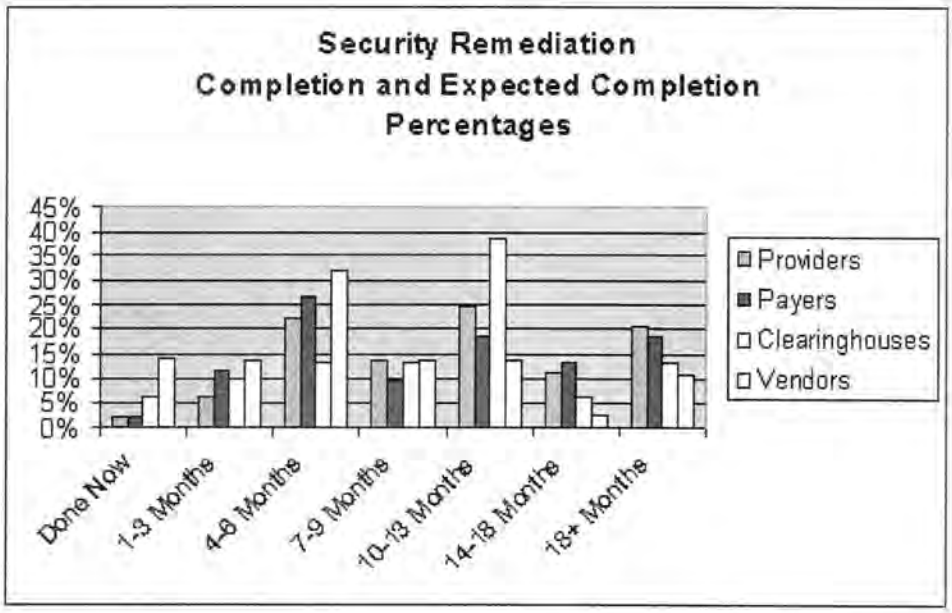
Only 5% of payers and providers reportedly have completed transactions/code sets remediation: Most respondents plan to complete efforts within one year, with nearly all estimating completion by the transactions deadline in 2003. However, 35% of providers and 26% of payers do not plan to complete their transactions remediation tasks by April 2002, and so, presumably will not meet HHS' deadline for beginning transactions testing.



Relatively little progress has been made in Privacy remediation implementation since July, though most respondents still predict that they will complete remediation by the April 2003 compliance deadline (consistent with our Spring and Summer 2002 Survey reports). However, concrete evidence of compliance is slim: only 5% of providers and 4% of payers have thus far completed their Privacy implementations. Further, less than 20% of providers and payers expect to finish in the next three months, bringing most essentially "down to the wire" in meeting the April 2003 Privacy deadline.



Respondents indicated that Security remediation efforts are progressing slowly; most don't predict completion for a year or more. The majority of organizations reportedly are still involved in the Security gap/risk analysis phase; vendors have made the most progress with about 45% reporting that implementation efforts are underway.



Provider Perceptions of Trading Partner Readiness

Based on their communications (or lack thereof) with payers, vendors and clearinghouses, many providers were skeptical that their trading partners would be ready to transmit HIPAA transactions by required deadlines. Most provider participants (74%) predicted that their clearinghouses would be ready, but 80% predicted that many, if not most, of their payers would NOT be able to meet the Transactions Rule deadlines; over 60% had the same concerns about vendor readiness.

USE OF OUTSIDE CONSULTANTS

Survey results for Fall 2002 showed that fewer respondents across the industry are currently using outside consultants to support HIPAA initiatives (43%) than during July (about 50%). The biggest users of consultants are larger hospitals (53%) and payers (60%). Respondents indicated that consulting support is being used primarily for assessment and project planning.

Third Party Transaction Compliance Testing

About 25% of participants indicated that their organizations plan to use third party certification of their transactions capabilities, and about 20% will recommend that trading partners certify with a third party prior to sending transactions. Fewer (mostly smaller providers) indicated that they plan to perform their own testing with trading partners without using a third party certification service. Few plan to "require" trading partners to certify through a third party. With just six months left before the testing deadline, over 40% of respondents either did not know or had not planned their testing strategies.

HIPAA BUDGET HIGHLIGHTS

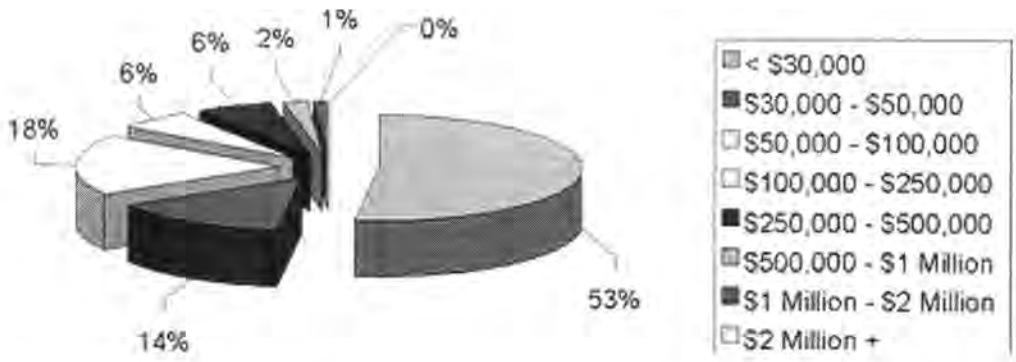
Hospital budgets for HIPAA compliance in 2003 are generally higher than 2002 HIPAA budgets. 40% of hospitals with less than 100 beds will spend less than $30K in 2003, just over 20% will spend between $30K and $50K, about 30% between $50K and $100K, and 7% between $100K and $250K. 25% of hospitals with 100 to 400 beds will spend less than $50K, 28% between $50K and $100K, 28% between $100K and $250K, 11% between 500K and $1 million, and 2% over $1 million. For hospitals with 400+ beds, 8% have budgeted between $30K and $50K, 13% between $50K and $100K, 25% between $100K and $250K, 20% between $250K and $500K, 20% between $500K and $1 million, 4% between $1 million and $2 million, and 8% $2 million+.
Payer and vendor budgets for 2003 are also slightly higher than 2002 budgets. A graphical comparison of hospital, payer and vendor HIPAA budgets, by year, is offered at the end of this report.

THE BIG PAYOFF?

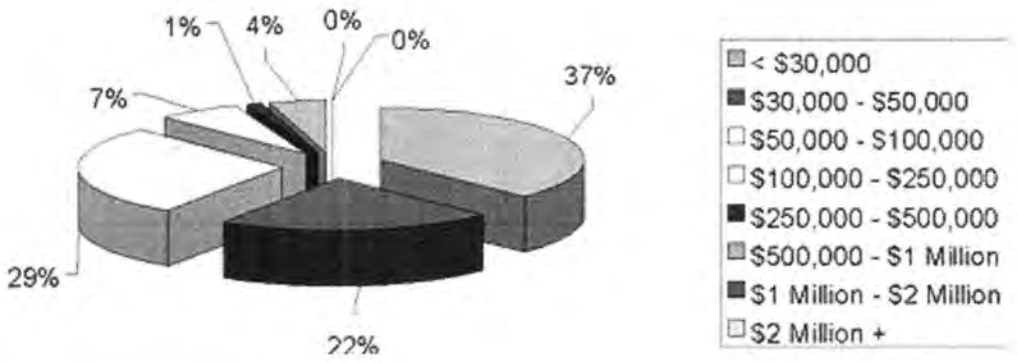
For the first time, we asked participants to focus on the "benefits" of HIPAA compliance. 56% of respondents reported that their organizations' strategic goals include realizing benefits from their HIPAA efforts, though 44% have not, as yet, focused on achieving HIPAA benefits. Participants identified prevention of future privacy/security breaches as the number one hoped-for benefit (78%), followed by increasing patient confidence through better privacy/security (67%). Providing a reminder of an original intent of HIPAA administrative simplification, the goal of saving time, effort and money through transactions standardization was identified by 62% of respondents, who indicated less optimism about the beneficial impact of implementing security and privacy measures (30%).

Hospital Budgets: 2002 vs. 2003

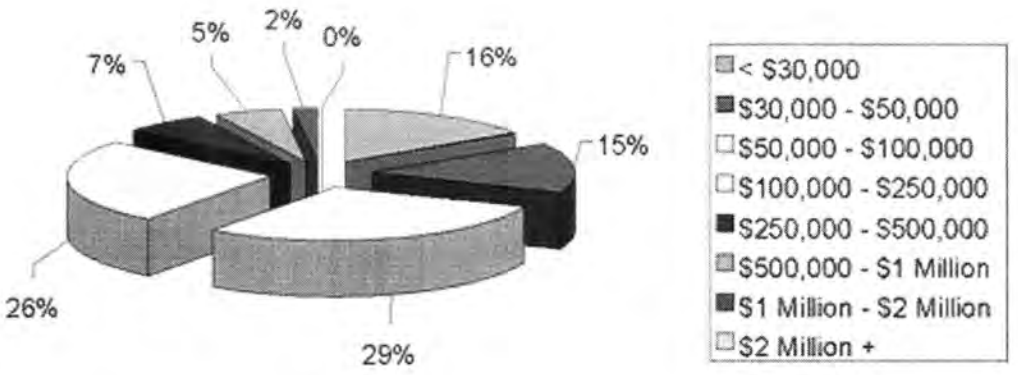
2002 Budgets
Hospitals with Less Than 100 Beds



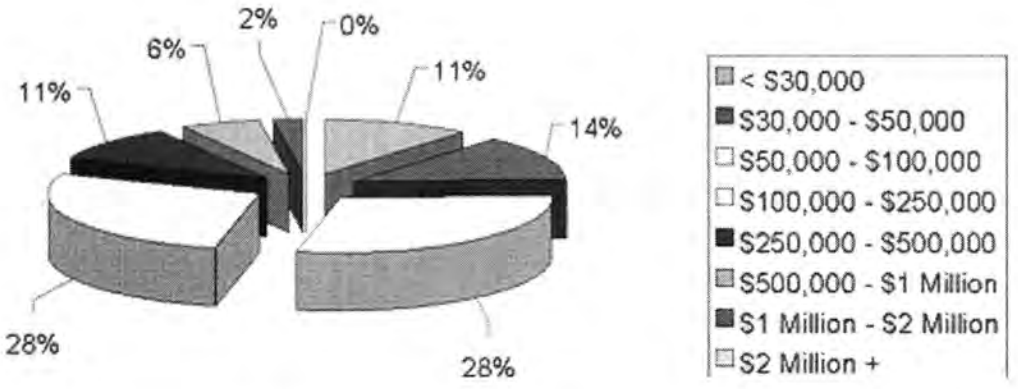
2003 Budgets
Hospitals with Less Than 100 Beds



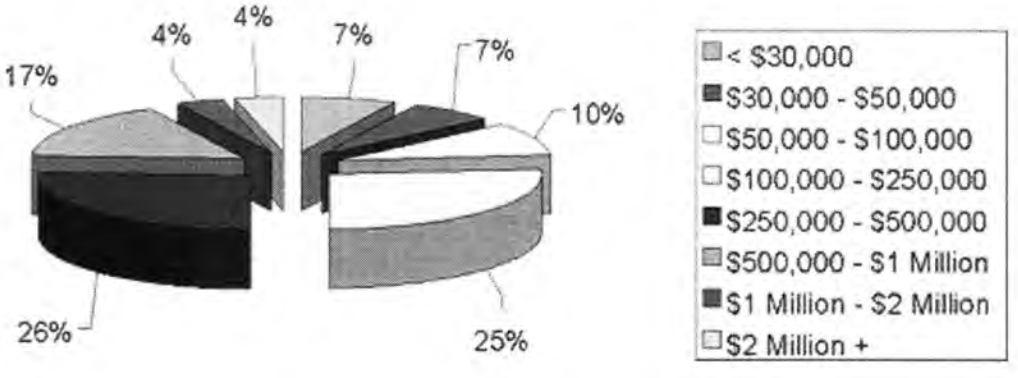
2002 Budgets
Hospitals with 100 to 400 Beds



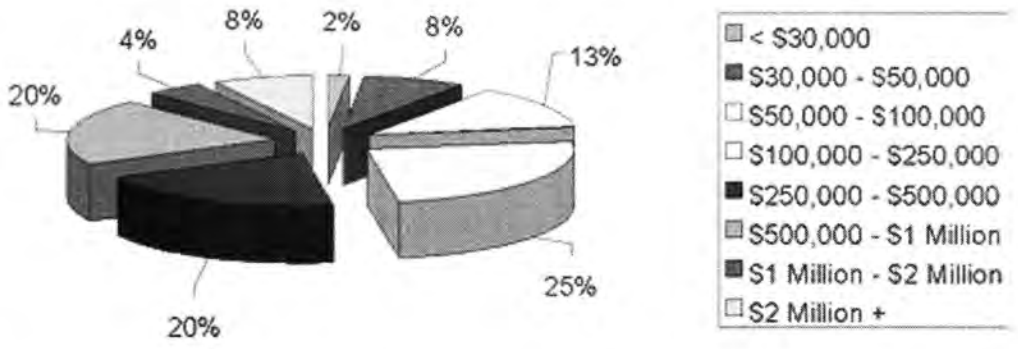
2003 Budgets
Hospitals with 100 to 400 Beds



2002 Budgets
Hospitals with 400 or More Beds

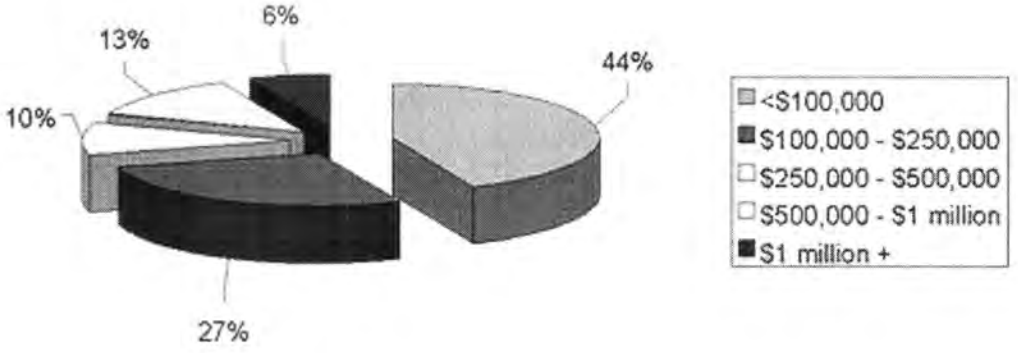


2003 Budgets
Hospitals with 400 or More Beds

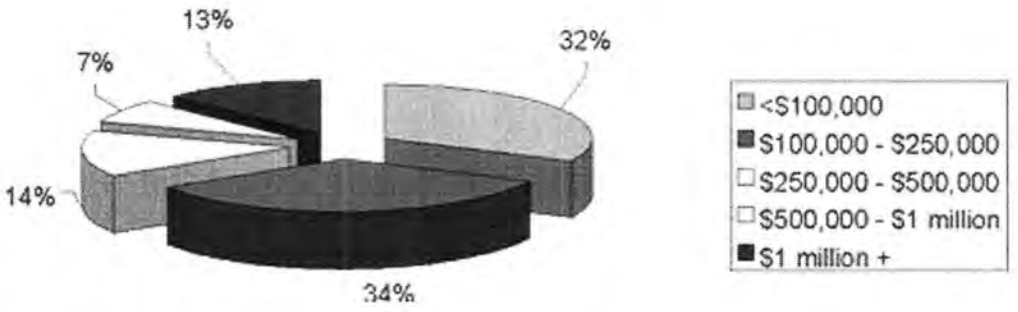


Payer Budgets: 2002 vs. 2003

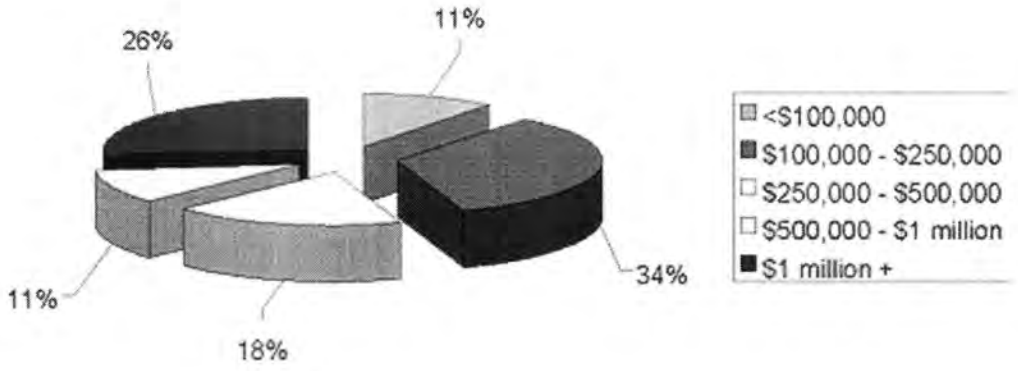
2002 Budgets
Payers Covering 150,000 or Fewer Lives



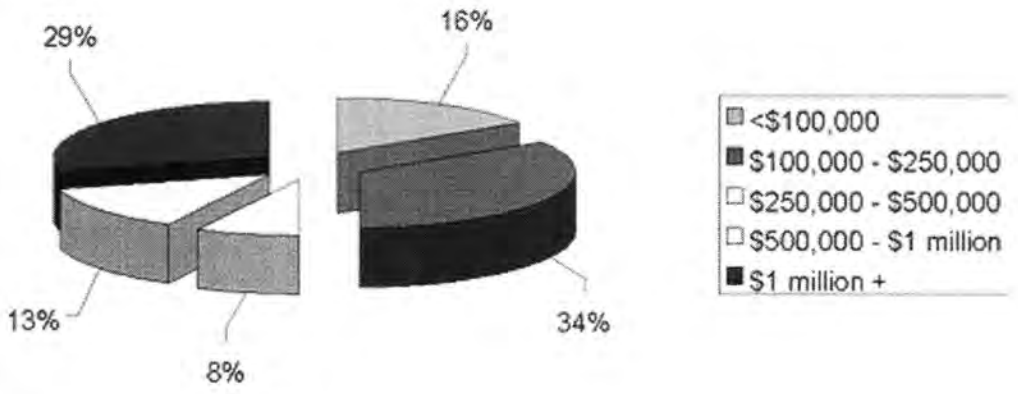
2003 Budgets
Payers Covering 150,000 or Fewer Lives



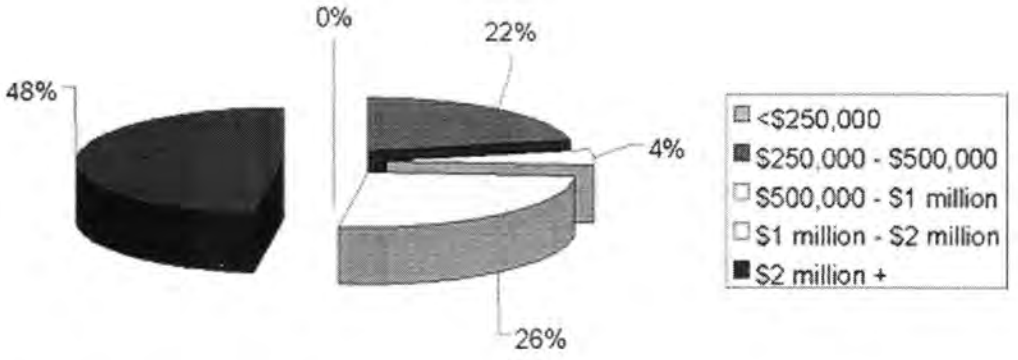
2002 Budgets
Payers Covering 150,000 to 500,000 Lives



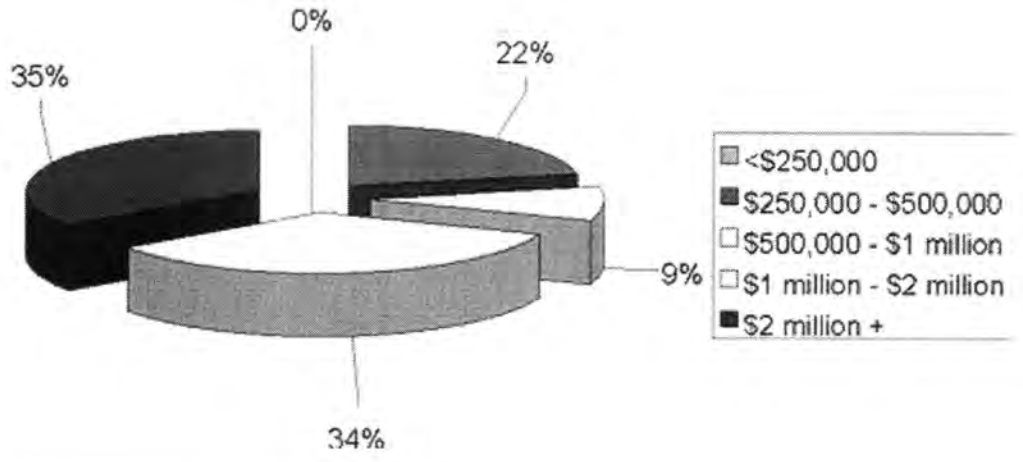
2003 Budgets
Payers Covering 150,000 to 500,000 Lives



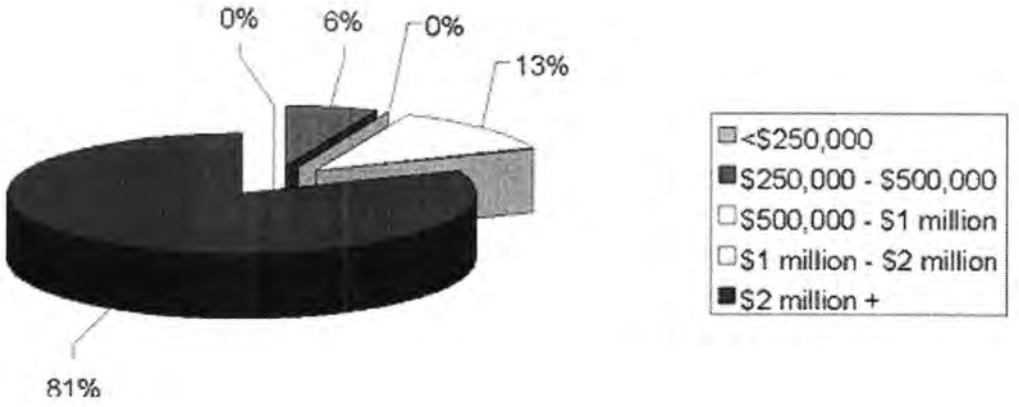
2002 Budgets
Payers Covering 500,000 to 1.5 Million Lives



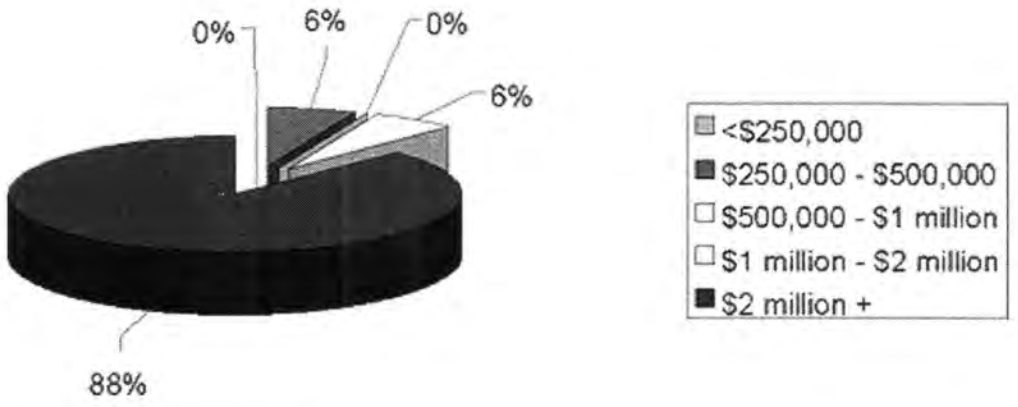
2003 Budgets
Payers Covering 500,000 to 1.5 Million Lives



2002 Budgets
Payers Covering More Than 1.5 Million Lives

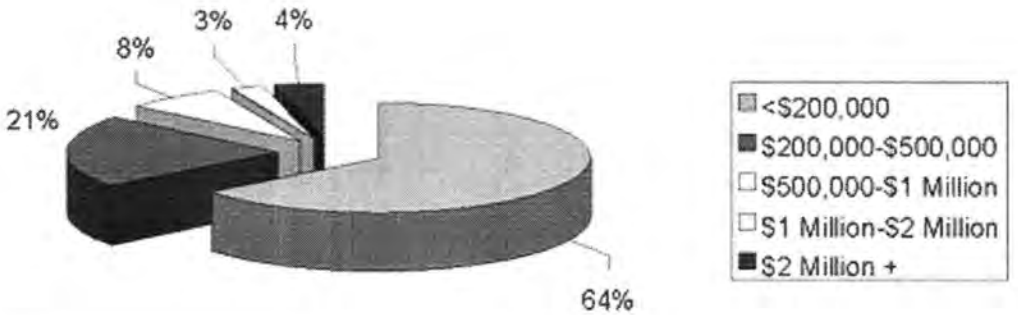


2003 Budgets
Payers Covering More Than 1.5 Million Lives



Vendor Budgets: 2002 vs. 2003

2002 Budgets
Vendors



2003 Budgets
Vendors